Einsatz von IT-GRC Funktionen in führenden ITSM Lösungen - Möglichkeiten und Grenzen

Bachelorarbeit

im Studiengang

Wirtschaftsinformatik

vorgelegt von

Egzon Murtaj

Matrikelnummer: 15535974

egzon.murtaj@gmail.com

am 22. Mai 2019

an der ZHAW School of Management and Law

betreut von

Dr. Christian Russ

Management Summary

Immer mehr IT-Organisationen konkurrieren sich um IT-Services, weshalb sich der Wettbewerb um die IT erhärtet und die Notwendigkeit für ITSM steigt. Gleichzeitig steigt auch die Komplexität von IT-Organisationen mit der sich erhöhenden Anforderung im Bereich der Transparenz, der Messbarkeit, der Kontrolle und der Nachvollziehbarkeit, weshalb IT-GRC an Bedeutung gewinnt. Eine Möglichkeit, Abhilfe gegen die steigenden Anforderungen zu schaffen, liegt im Einsatz von IT-GRC Funktionen in ITSM Lösungen.

Es lässt sich die zentrale Forschungsfrage ableiten, welche Möglichkeiten und Grenzen zum Einsatz von IT-GRC Funktionen in ITSM Lösungen bestehen. Zur Beantwortung der zentralen Forschungsfrage stellen sich die weiteren Teilfragen, welche Berührungspunkte ITSM und IT-GRC aufweisen, welche führenden ITSM Lösungen am Markt angeboten werden, welche Bewertungskriterien den Einsatz von IT-GRC Funktionen in ITSM Lösungen messen, wie führende ITSM Lösungen abschneiden und welche Mächtigkeit sowie Limitation sich daraus ergeben.

Die Bachelorarbeit baut auf Wissen von Literatur und Experteninterviews auf. Durch dieses Wissen werden zuerst die theoretischen Grundlagen von ITSM, IT-GRC und jener der Berührungspunkte beider Themengebiete durchleuchtet und in einem Venn-Diagramm visualisiert. Eine Marktanalyse identifiziert die führenden ITSM Lösungen und ein Bewertungskatalog definiert die Kriterien zur Evaluierung vom Einsatz von IT-GRC Funktionen in ITSM Lösungen. Eine Nutzwertanalyse zeigt auf Basis des Bewertungskatalogs und die Ergebnisse der Evaluierung auf, um daraus die Mächtigkeit und Limitation abzuleiten.

ITSM kann als Werkzeug für IT-GRC dienen, indem die Aufgaben eines Risk Managements und Compliance Managements in ITSM Lösungen funktional abgebildet werden. Aus der Marktanalyse von ITSM Lösungen resultieren Cherwell Software, Ivanti und ServiceNow als führende ITSM Lösungsanbieter, welche anhand eines Bewertungskatalogs von insgesamt 15 Kriterien evaluiert werden. Die Evaluierung zeigt, dass sowohl in der Qualität als auch in der Quantität die ITSM Lösung von ServiceNow im Einsatz von IT-GRC Funktionen führt. Die ITSM Lösung von Cherwell Software folgt der ITSM Lösung von ServiceNow dicht, wobei die ITSM Lösung von Ivanti noch Verbesserungspotenziale für den Einsatz von IT-GRC Funktionen birgt.

Auf der einen Seite bestehen die Möglichkeiten zum Einsatz von IT-GRC Funktionen in führenden ITSM Lösungen sowohl in der Qualitätsverbesserung als auch in der Senkung der Dauer und der Aufwandsreduktion von IT-GRC relevanten Prozessen. Auf der anderen Seite liegen die Grenzen in den initial hohen Kosten, der rasch zunehmenden Komplexität im Detaillierungsgrad und den automatisierten Messungen in Prozessen, die in der ITSM Lösungen nicht abgebildet werden können. Da sich ITSM Lösungen immer mehr zu ESM Lösungen wandeln, besteht jedoch Potenzial für die Ausweitung der abgebildeten Prozesse und somit für den Einsatz von IT-GRC Funktionen. Als zentrale Handlungsempfehlung definiert sich ein Abgleich der Möglichkeiten und Grenzen, woraus eine Gewichtung für die Nutzwertanalyse resultieren soll.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

CCO	Chief Compliance Officer
CIO	Chief Information Officer
CMS	Configuration Management System
COBIT	Control Objectives for Information and Related Technology
CSM	Cherwell Software Management
CSV	Comma Separated Values
EGIT	Enterprise Governance of Information and Technology
ESM	Enterprise Service Management
GDPR	General Data Protection Regulation
IKS	Internes Kontrollsystem
I&O	IT Infrastructure and Operations
ISM	Ivanti Service Manager
ISMS	Information Security Management System
IT-GRC	IT-Governance, Risk and Compliance
ITIL	IT-Infrastructure Library
ITSM	IT-Service Management
mApp	Mergeable Application
SaaS	Software as a Service
SLA	Service Level Agreement
UCF	Unified Compliance Framework

1 Einleitung

Die Einleitung schildert mit der Ausgangslage den aktuellen Standpunkt von IT-Governance, Risk and Compliance (IT-GRC) und IT-Service Management (ITSM), um das Forschungsinteresse der Thematik darzulegen. Basierend auf das Forschungsinteresse wird die zentrale Forschungsfrage definiert, aus welcher sich weitere Teilfragen zur Beantwortung der zentralen Forschungsfrage stellen. Nach einer Abgrenzung der Bachelorarbeit wird das methodische Vorgehen und der Aufbau zur Beantwortung aller Forschungsfragen erläutert.

1.1 Ausgangslage

In einer Studie der KPMG Schweiz wurden gemäss Arikan (2018) 88% der befragten Unternehmen in den letzten 12 Monaten Opfer von Cyberattacken. Im Vergleich zum Vorjahr nahm die Opferzahl um 34 Prozentpunkte zu (Arikan, 2018). Damit verbunden nehmen die Aufgaben des Risk-Management kontinuierlich zu. Neben den zunehmenden Risiken steigen auch mit jeder neuen Gesetzgebung die Aufwände für Compliance-Tätigkeiten innerhalb von Unternehmen (Schweizer, 2017). Ein aktuelles Beispiel wiederspiegelt die General Data Protection Regulation (GDPR) der EU vom 25. Mai 2018. Bei Verstossen drohen den Unternehmen Bussen von bis zu vier Prozent des Jahresumsatzes oder maximal 20 Millionen Euro (Heiniger, 2018). Insgesamt erhöhen die steigenden Anforderungen im Bereich der Transparenz, der Messbarkeit, der Kontrolle und der Nachvollziehbarkeit die Notwendigkeit und die Wichtigkeit von IT-GRC.

Gleichzeitig ist IT-Infrastructure Library (ITIL)-basiertes ITSM ein richtungsweisendes Thema in den IT-Führungsetagen nationaler und internationaler Konzerne. ITSM ist das Resultat der Orientierung von IT-Organisationen an die flexiblen Bedürfnisse der Kunden. Für eine IT Organisation zeigt sich die Anbindung von ITIL in ihrem ITSM dadurch vorteilhaft, dass eine klare Regelung der Verantwortlichkeiten überhaupt die Kompetenzen definiert, Reaktionsgeschwindigkeiten erhöht werden, eine Basis für Outsourcing von IT-Teilbereichen geliefert wird, messbare Leistungsindikatoren eine einfachere Steuerung ermöglichen oder eine neue Service Kultur geschaffen wird (Brandstätter & Peruzzi, 2006, S. 266). Durch die Ausrichtung von IT-Organisationen an Kundenanforderungen nimmt die Komplexität der IT-Organisationen zu. Können IT-GRC Funktionen in ITSM Lösungen Abhilfe schaffen, um die steigenden Anforderungen an Transparenz, Messbarkeit, Kontrolle und Nachvollziehbarkeit effizienter zu behandeln?

1.2 Forschungsfragen

Die Zielsetzung dieser Bachelorarbeit ist, die Unterstützung von IT-GRC Funktionen in führenden ITSM Lösungen zu erforschen und daraus die Möglichkeiten sowie Grenzen abzuleiten. Online-Recherchen am Publikationsdatum dieser Bachelorarbeit zeigen, dass sowohl ITSM als auch IT-GRC nachgefragte Themen sind. Im Gegensatz sind nach Online-Recherchen die Überschneidungen beider Themen wissenschaftlich wenig erschlossen. Zum Einsatz von IT-GRC Funktionen in ITSM Lösungen lassen sich keine wissenschaftlichen Studien finden und es besteht somit eine Wissenslücke. Gestützt auf die Zielsetzung und das Forschungsinteresse lautet die zentrale Forschungsfrage der Bachelorarbeit wie folgt:

- *Welche Möglichkeiten und Grenzen bestehen für den Einsatz von IT-GRC Funktionen in führenden ITSM Lösungen?*

Zur Bearbeitung der zentralen Forschungsfrage stellen sich die folgenden fünf Teilfragen:

1. *Welche Berührungspunkte weisen ITSM und IT-GRC auf?*
2. *Welche führenden ITSM Lösungen werden am Markt angeboten?*
3. *Welche Bewertungskriterien messen den Einsatz von IT-GRC Funktionen in ITSM Lösungen?*
4. *Wie schneiden führende ITSM Lösungen ab?*
5. *Welche Mächtigkeit und Limitation werden abgeleitet?*

1.3 Abgrenzung

Die Anforderungen an ITSM Lösungsanbieter steigen mit den sich stetig verändernden Bedürfnissen der Kunden (Pröhl & Zarnekow, 2019). Entsprechend evaluiert die Bachelorarbeit die am Publikationsdatum angebotenen ITSM Lösungen beziehungsweise deren Funktionen zum Einsatzgebiet von IT-GRC. In der Evaluierung werden international führende ITSM Lösungsanbieter berücksichtigt. Für die theoretische Grundlagen dienen sowohl die Version ITIL V3 2011 als auch die Version COBIT 5. In der Zwischenzeit wurde für beide Frameworks eine neuere Version entwickelt. Da sich die ITSM Lösungsanbieter noch erst einarbeiten und anpassen müssen, reichen die Versionen ITIL V3 2011 sowie COBIT 5 als Grundlagen dieser Bachelorarbeit aus.

1.4 Methodisches Vorgehen und Aufbau

Im Grundsatz wählt die Bachelorarbeit die Methodik der Nutzwertanalyse und beabsichtigt, ein Artefakt in Form einer Nutzwertgewichtung der führenden ITSM Lösungen zum Einsatz von IT-GRC Funktionen zu erstellen. Die Nutzwertgewichtung dient potenziellen Kunden, die Gewichtung der Bewertungskriterien den eigenen Bedürfnissen auszurichten und damit die Auswahl einer ITSM Lösung mit dem Fokus auf IT-GRC Funktionen durch diese Bachelorarbeit zu belegen. Gleichzeitig werden die Mächtigkeit und Limitation der einzelnen ITSM Lösungsanbieter in Bezug auf die angebotenen IT-GRC Funktionen erforscht, um mögliche Verbesserungspotenziale festzustellen. Das methodische Vorgehen der Bachelorarbeit ist in sechs Kapitel aufgeteilt, wobei *Kapitel 1* die Einleitung bildet.

Kapitel 2 beleuchtet sowohl mit der Definition von ITSM und IT-GRC als auch mit deren Berührungspunkten die Theorie. Im ersten Kapitel richtet sich das Vorgehen der Bachelorarbeit auf die Ausarbeitung vorhandener Literatur, wo zuerst die Begrifflichkeiten von ITSM und IT-GRC sowie ihre Ausprägungen definiert werden. In einem zweiten Schritt werden die Berührungspunkte von ITSM und IT-GRC ermittelt und als Venn-Diagramm modelliert, um gepaart mit der Definition die theoretische Grundlage zu untermauern. Neben der Ausarbeitung vorhandener Literatur fliessen in diesem Kapitel Experteninterviews ein, um mit dem Expertenwissen die theoretischen Grundlagen zu erschliessen und zu festigen. Im Rahmen der Bachelorarbeit wurden die Experten André Frensel, Kurt Stuber, Marco Brügger und Stefan Jung konsultiert. André Frensel ist ITSM Business Consultant sowie Geschäftsführer der nextEDGE Business Consulting GmbH und weist langjährige Erfahrung in der Beratung auf. Kurt Stuber ist ITIL Experte und über mehrere Jahre als Consultant im ITSM Bereich und darüber hinaus tätig. Marco Brügger ist Partner von sevida und langjährig in den Bereichen Risk Management und Security spezialisiert. Stefan Jung berät Unternehmen freiberuflich als Projekt Manager, ITIL Experte sowie IT Consultant und weist langjährige Erfahrung in der Beratung dieser Bereiche auf. Das Ziel vom Kapitel 2 ist die Durchleuchtung der ersten Teilfrage *"Welche Berührungspunkte weisen ITSM und IT-GRC auf?"*.

Kapitel 3 führt eine Marktanalyse durch, aus der drei ITSM Lösungsanbieter selektiert werden. Die Möglichkeiten und Grenzen von IT-GRC in ITSM sollen mithilfe von Lösungen aufgezeigt werden, welche am Markt angeboten und in Unternehmen angewendet werden. Daraus ergibt sich die Notwendigkeit, am Markt angebotene ITSM Lösungen zu eruieren. Die Selektion drei führender ITSM Lösungen erfolgt unter der Rücksichtnahme

der Bereitschaft des ITSM Lösungsanbieters, Hands-On-Demos und Testzugänge zu ermöglichen. Damit wird die zweite Teilfrage *"Welche führenden ITSM Lösungen werden am Markt angeboten?"* beantwortet.

Kapitel 4 arbeitet einen Bewertungskatalog zur Evaluierung von IT-GRC Funktionen in ITSM Lösungen aus. Zur Bewertung der IT-GRC Funktionen in den einzelnen ITSM Lösungen wird die Methodik der Nutzwertanalyse eingesetzt. Um eine Nutzwertanalyse durchzuführen, bedarf es eine Ausarbeitung eines Bewertungskatalogs, in welcher die Bestimmung der Bewertungskriterien einfliesst und damit die dritte Teilfrage *"Welche Bewertungskriterien messen den Einsatz von IT-GRC Funktionen in ITSM Lösungen?"* behandelt wird. Die Bewertungskriterien werden mithilfe von Experteninterviews und wissenschaftlichen Artikeln ausgearbeitet. Die Experteninterviews werden in diesem Kapitel einbezogen, um die kritischen, funktionalen Bewertungskriterien für den Einsatz von IT-GRC Funktionen in ITSM Lösungen zu ernennen.

Kapitel 5 leitet zu den Evaluierungen über, wo die drei führenden ITSM Lösungen einzeln zum Einsatz von IT-GRC Funktionen untersucht werden. Das Anwendungsgebiet der Evaluierung umfasst Produktdokumentationen, Hands-On-Demos und Testzugänge. Das Ziel dieses Kapitels ist, tiefe Einblicke über den Einsatz von IT-GRC Funktionen in den jeweiligen ITSM Lösungen zu gewinnen. Durch die Evaluierung wird der Grundstein für die Bearbeitung der vierten Teilfrage *"Wie schneiden führende ITSM Lösungen ab?"* gelegt. Eine zentrale Anforderung für die darauffolgende Analyse ist, dass eine möglichst gleiche Informationsqualität über jede ITSM Lösung besteht.

Kapitel 6 führt die Nutzwertgewichtung für die einzelnen ITMS Lösungen durch. Die einzelnen ITSM Lösungen werden auf die Einsatzfähigkeit von IT-GRC Funktionen bewertet. Es entsteht eine Nutzwertgewichtung, welche als Ausgangspunkt zur Beurteilung der Forschungserkenntnisse dient. Die Forschungserkenntnisse sollen darlegen, welche Mächtigkeit die einzelnen ITSM Lösungen zu IT-GRC aufweisen. Es folgt eine kritische Betrachtung über die Limitation der ITSM Lösungsanbieter, unter anderem ob angepriesene Funktionen realitätstauglich sind. Mit der Lösung der fünften und letzten Teilfrage *"Was ist die Mächtigkeit und Limitation von IT-GRC Funktionen in ITSM Lösungen?"* wird gleichzeitig die zentrale Forschungsfrage der Bachelorarbeit *" 5. Welche Mächtigkeit und Limitation werden abgeleitet?"* eruiert.

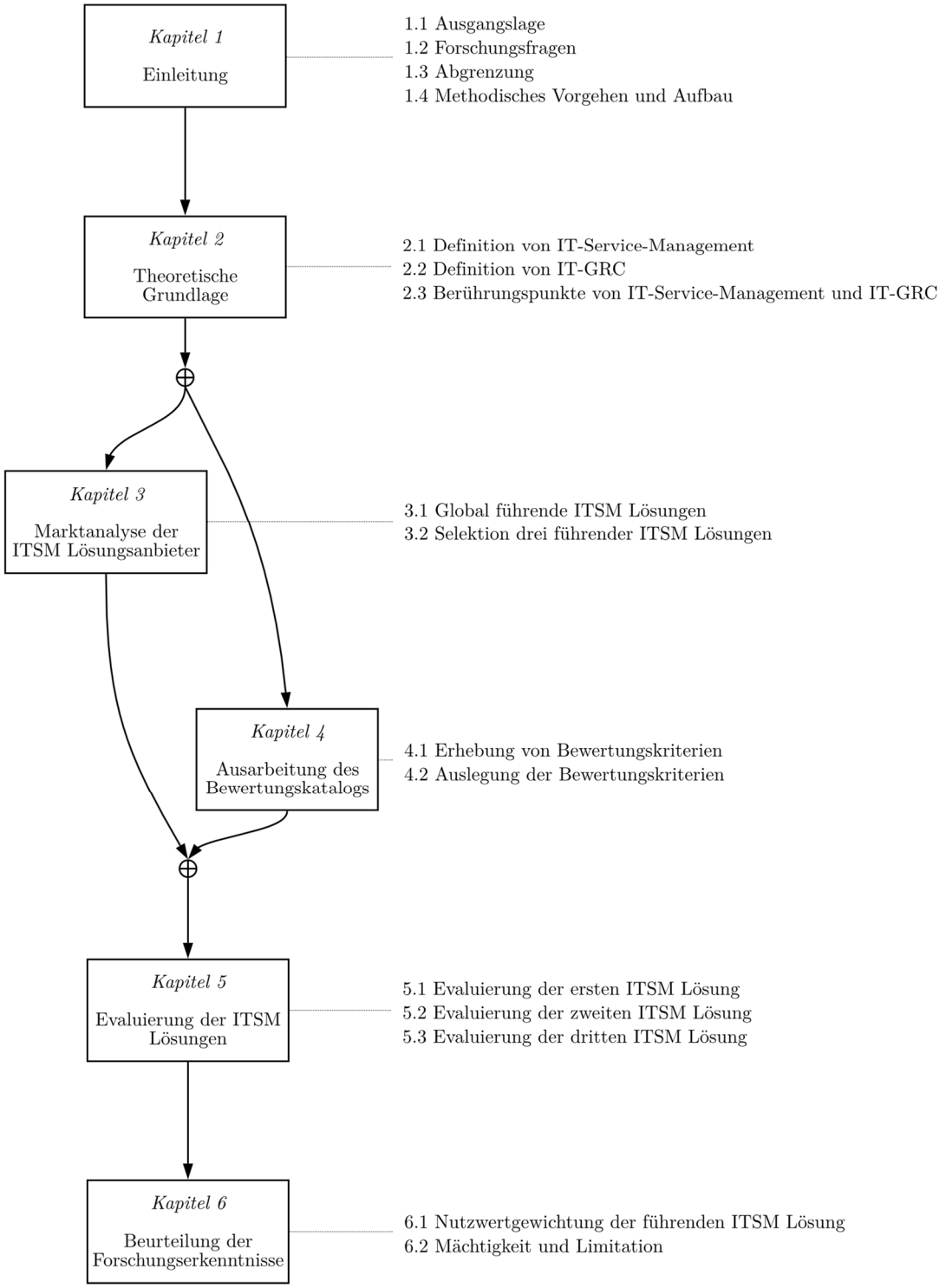


Abbildung 1: Aufbau der Bachelorarbeit

2 Theoretische Grundlage

Sowohl ITSM als auch IT-GRC haben sich in Lehrbüchern, Frameworks und Organisationen etabliert. Heute ist ITSM in IT-Organisationen fast unvermeidlich und IT-GRC hat sich als ein geeigneter Lösungsansatz für die strategische Steuerung von IT-Organisationen verbreitet (Racz, Weippl, & Seufert, 2010, S. 106). Dieses Kapitel durchleuchtet die Theorie und beinhaltet in einem ersten Schritt sowohl die Definitionen von ITSM als auch von IT-GRC. In einem zweiten Schritt werden die Berührungspunkte zwischen ITSM und IT-GRC ermittelt, erläutert und als Venn-Diagramm abgebildet.

2.1 Definition von ITSM

In den letzten 100 Jahren hat sich in den Industrieländern eine deutliche Verschiebung vom Primär- und Sekundärsektor zum Tertiärsektor vollzogen (Hanudelova & Prochazkova, 2018, S. 177). Der Tertiärsektor kennzeichnet sich hauptsächlich durch die Erbringung von Dienstleistungen anstelle von der Herstellung von Produktionsgütern (Hanudelova & Prochazkova, 2018, S. 177). Die Dienstleistungen der Informationstechnologie, welche IT-Services genannt werden, sind das Fundament des Themengebiets von ITSM (Teubner & Remfert, 2017, S. 451). IT-Service Provider erbringen IT-Services, welche von internen oder externen Kunden beauftragt werden und für die gemäss der Experteninterviews in der Regel eine geschäftliche Notwendigkeit für den Einsatz von IT-Services besteht, wie beispielsweise zu Software- oder Netzwerklösungen. IT-Services bieten dem Kunden zeit-, kosten- und qualitätsoptimal einen Mehrwert mit der Eigenschaft, dass sich gemäss der Experteninterviews und nach Rouhani (2017, S. 730) der Kunde von spezifischen Kosten und Risiken fernhalten kann.

Zu Beginn des Einzugs der IT dienten IT-Services lediglich zur Unterstützung von Geschäftsprozessen, wobei mit der fortschreitenden Digitalisierung die Nachfrage sowie die Wichtigkeit an IT-Services stieg und IT-Services immer öfter als Business Enabler und Innovator überhaupt Geschäftstätigkeiten ermöglichen (Wiedenhofer, 2017, S. 53). 73% aller von Böhm, Müller, Krcmar und Welpe (2018, S. 41) befragten Unternehmen sind der Überzeugung, dass sich immer mehr Provider um IT-Services konkurrieren und sich der Wettbewerb um die IT deshalb erschwert. Es steigen sich somit die Möglichkeiten für Unternehmen, strategisch unwichtige IT-Services günstiger von externen anstelle von internen IT-Service Providern zu beziehen. Da aufgrund der strategischen Relevanz ein Outsourcing nicht für alle IT-Services in Frage kommt und beim Outsourcing nach

Lindner und Leyh (2019) neben dem Vorteil der Skalierbarkeit hingegen das Risiko steigt, keinen Einfluss auf die Qualität der IT-Services zu nehmen, verbleiben IT-Services weiterhin inhouse. Wiedenhofer (2017, S. 54) hält die Anforderungen fest, dass interne IT-Organisationen immer mehr die Qualität der IT-Services zu verbessern und zeitgleich die IT-Services mit einem tieferen Aufwand bereitzustellen haben.

2.1.1 ITSM als Disziplin von IT-Organisationen

ITSM knüpft an den Zielkonflikt zwischen der Qualitäts- und Aufwandsanforderungen an die IT-Organisation und strebt die Stärkung der Kundenorientierung, die Optimierung der Kostenkontrolle und weitere Nutzenpotenziale für IT-Services durch das Zusammenführen von Prozessmanagement und branchenspezifischen Best Practices an (Rouhani, 2017, S. 730). Söllner und Drescher (2019) erörtern, dass ITSM einem Service- und Prozessdenken nacheifert und das Prinzip

> *"Ein Bauer verkauft Äpfel auf einem Markt. Schöne, saftige Äpfel. Ein Bäcker hat Apfelkuchen im Angebot, der sehr populär ist, und ist auf der Suche nach einem Lieferanten. Ausserdem möchte er nicht einfach nur Äpfel, sondern regelmässige Lieferungen von bestimmten Mengen, auf die er sich verlassen kann, zu bestimmten Zeitpunkten geliefert bekommen, so dass er immer genug Apfelkuchen für seine Kunden backen kann."*

wiederspiegelt. Zwischenzeitlich hat sich ITSM zu einer zentralen Komponente für den Erfolg oder Nichterfolg von IT-Organisationen klassifiziert (Söllner & Drescher, 2019). Beispielsweise regelt ITSM Vereinbarungen zu IT-Services zwischen dem Kunden und dem Provider in Service Level Agreements (SLA) durch ein Service Level Management (Schomann & Röder, 2008, S. 326). Das ITSM behandelt Störungen von IT-Services im Incident Management und bei wiederholenden Störungen im Problem Management. Weiter treten in Verbindung mit ITSM unter anderem die Begriffe Request Fulfilment, Event Management oder Access Management auf, die im Tagesgeschäft einer IT-Organisation anzutreffen sind. Dadurch, dass gemäss der Experteninterviews die Definition von ITSM aus Best-Practice Framework entnommen werden kann und sich viele Unternehmen an Frameworks wie ITIL zur Definition, Planung, Implementierung, Ausführung und Optimierung von IT-Services stützen, wird ITIL als Framework und als theoretische Grundlage für ITSM im nächsten Kapitel erläutert.

2.1.2 ITIL V3 2011 als Framework für ITSM

Für ITSM hat sich ITIL V3 2011 branchenübergreifend etabliert und ist gefolgt von COBIT 5 das Framework mit der weltweit höchsten Akzeptanzrate in IT-Organisationen (Marrone & Kolbe, 2011, S. 5 f.). Die hohe Akzeptanz lässt sich darauf stützen, dass ITIL V3 2011 die IT nicht nur als Technologie, sondern als Mittel zur Erbringung von Services für Kunden interpretiert. Das Good-Practice-Framework ITIL V3 2011 umschliesst eine Sammlung von Best-Practice-Ansätzen von bewährten Praktiken und Erfahrungen weltweit führender Service Provider. Obwohl nach Teubner und Remfert (2017, S. 455) ITIL V3 2011 die "*industrielle Produktion*" von IT-Services nicht explizit als Definitionsmerkmal hervorhebt, wird dieses Merkmal oft in der Wissenschaft verwendet. Dadurch, dass ITIL V3 2011 neutral und unabhängig von Herstellern ist, können bewährte Praktiken auf die verschiedenen Bedürfnisse der IT-Organisationen adaptiert werden. Die Services durchlaufen in ITIL V3 2011 gemäss der Abbildung 2 ein Lebenszyklus. Der Servicelebenszyklus beinhaltet 26 Kernprozesse und ist in den fünf Phasen beziehungsweise Büchern *Service Strategy* von Cannon (2011), *Service Design* von Hunnebeck (2011), *Service Transition* von Rance (2011), *Service Operation* von Rance (2011) und *Continual Service Improvement* von Lloyd (2011) beschrieben.

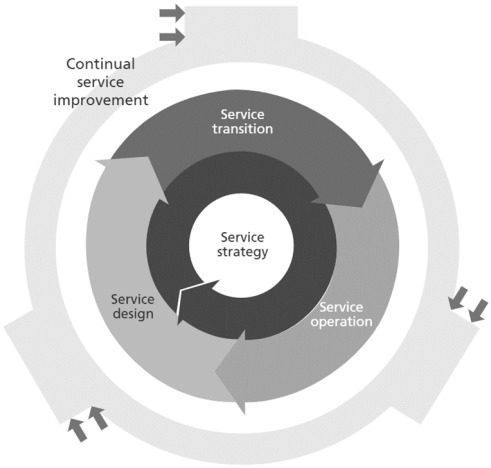


Abbildung 2: ITIL V3 2011 Servicelebenszyklus (Cannon, 2011; Hunnebeck, 2011; Lloyd, 2011; Rance, 2011; Steinberg, 2011)

Im Jahr 2019 ist die neuere Version namens ITIL 4 erschienen, welches umso mehr gemäss Spalding (2019) die Silos in IT-Organisationen unter anderem mit einem Service Value System und Service Value Chain anstelle des Servicelebenszyklus und mit 34 Practices anstelle der 26 Kernprozesse aufbrechen soll. Da in der Wirtschaft die verschiedenen Lösungen erst an ITIL 4 adaptiert werden müssen, dient ITIL V3 2011 als theoretische Grundlage für ITSM.

Die Service-Strategy-Phase definiert gemäss Cannon (2011) die Strategie zur Erbringung von IT-Dienstleistungen beziehungsweise von IT-Services für Kunden. Basierend auf internen und externen Faktoren, namentlich dem Business, dem Kunden, der Konkurrenz und weiterer Anspruchsgruppen, bestimmt die Service-Strategy-Phase die Ziele des IT-Service Providers und legt fest, wie diese Ziele zu erreichen sind. Zentral für die Service-Strategy-Phase sind die vier Ps: *Perspective*, *Position*, *Plan* und *Pattern*. "*Perspective*" dient zur Bestimmung der Perspektive, "*Position*" zur Positionierung im Markt, "*Plan*" zur Ausarbeitung eines Plans und "*Pattern*" zur Implementierung von Handlungsmustern. Die Umsetzung der vier Ps ermöglichen die Kernprozesse der Service-Strategy-Phase bestehend aus dem Strategy Management for IT-Services, Service Portfolio Management, Financial Management for IT-Services, Demand Management und Business Relationship Management. Das Strategy Management for IT-Services sichert aus der Sicht des Business die Entwicklung, Nutzung und Verbesserung der IT-Strategie durch eine definierte und kommunizierte Vision sowie Mission. Auch ist für das Strategy Management for IT-Services eine klare Marktpositionierung von hoher Bedeutung. Das Service Portfolio Management verwaltet das Serviceportfolio, um mit Investitionen und der richtigen Auswahl von anzubietenden IT-Service die maximale Wertschöpfung sowie minimale Risiken und Kosten zu erzielen. Das Serviceportfolio dient als Überblick aller IT-Services während des gesamten Lebenszyklus. Das Financial Management for IT-Services befasst sich mit der Servicebewertung, Finanzplanung, Kostenrechnung und Leistungsverrechnung von IT-Services. Das Demand Management prüft die Nachfrage der Kunden und gleicht damit das Angebot ab. Das Business Relationship Management betreut die Kunden, erhält das Verhältnis zu den Kunden aufrecht oder holt die Anforderungen der Kunden ab, um schlussendlich die Kundenzufriedenheit und -bindung zu erhöhen (Cannon, 2011).

Die Service-Design-Phase plant gemäss Hunnebeck (2011) IT-Services auf Basis von kundenspezifischen Anforderungen. Die Service-Design-Phase ist für die Entwicklung neuer IT-Services sowie für die Verbesserung bestehender IT-Services verantwortlich. IT-Services unterscheiden sich in ihrer Art als Core Service, Enabling Service und Enhancing Service und werden in verschiedener Kombination als Service Design Package für interne oder externe Kunden zur Verfügung gestellt. Die Kernprozesse zur Entwicklung neuer IT-Services sind die Design Coordination, das Service Catalogue Management, Service Level Management, Availability Management, Capacity Management, Service Continuity Management, Information Security Management und Supplier Management. Die Design Coordination koordiniert die Service-Design-Phase bei der Erfüllung

der Vorgaben der Service Strategy. Das Service Catalogue Management fasst einen Katalog aller IT-Services mit vollständigen Informationen zusammen und pflegt diesen regelmässig. Das Service Level Management verwaltet die SLAs, in denen Abmachungen mit den Kunden betreffend den IT-Services festgehalten werden. Das Capacity Management stimmt die Kapazität für das Erbringen der IT-Services in Bezug auf die Wirtschaftlichkeit ab und das Availability Management sichert die Verfügbarkeit von IT-Services, um das Minimum der Kundenanforderungen nicht zu unterschreiten. In Katastrophenfällen gewährleistet das Service Continuity Management den Betrieb von kritischen Business-Funktionen und sorgt für die Wiederherstellung des Normalzustands aller IT-Services. Das Information Security Management sichert die Geschäftsprozesse durch Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Nicht-Abstreitbarkeit, indem Risiken der Informationssicherheit identifiziert und durch Massnahmen behandelt werden. Im Supplier Management werden die externen Lieferanten gebündelt und die eingekauften Services gesteuert, um diese in der angemessenen Qualität in die eigenen IT-Services zu implementieren (Hunnebeck, 2011).

Die Service-Transition-Phase fokussiert sich gemäss Rance (2011) auf die Überführung von neuer oder geänderter IT-Services in produktive Systeme. Die Überführung wird mit allen nötigen Aufgaben geplant und verwaltet, um IT-Services reibungslos zu implementieren und Änderungen für die Nachvollziehbarkeit zu dokumentieren. Die Aufgaben der Service-Transition-Phase sind das Transition Planning & Support, Change Management, Service Asset & Configuration Management, Release & Deployment Management, Service Validation & Testing, Change Evaluation und Knowledge Management. Das Transition Planning & Support assistiert die Implementation neuer IT-Services in die Produktion durch die Planung und die Koordination der Ressourcen sowie die Sicherstellung der Integrität. Das Change Management steuert Veränderungen an IT-Services, indem negative Auswirkungen minimiert und die Veränderung effizient sowie effektiv durchgeführt wird. Das Service Asset & Configuration Management verwaltet Service-Assets und Configuration Items durch ein Configuration Management System (CMS). Als Service Assets werden das Leistungsvermögen beziehungsweise die Ressourcen der IT-Services und als Configuration Items die einzelnen Komponenten aller Ressourcen bezeichnet, die zur Erbringung der IT-Services einfliessen. Neben Softwarelösungen können zum Beispiel auch Dokumentationen oder auch Peripheriegeräte die Rolle eines Configuration Items übernehmen. Im CMS sind sowohl aktuelle als auch historische Informationen zu Service-Assets und Configuration Items konsistent hinterlegt. Im Release & Deployment

Management werden Releases in die Zielumgebung termingerecht und störungsfrei ausgerollt. Unter Service Validation & Testing wird die Qualität neuer oder veränderter IT-Services geprüft, damit die Qualität den Kundenanforderungen entspricht. Die Change Evaluation misst und beurteilt die aktuelle Performance. Das Knowledge Management bündelt und stellt Informationen für Entscheidungsorgane zur Entscheidungsfindung bereit (Rance, 2011).

Die Service-Operation-Phase stellt gemäss Steinberg (2011) den Betrieb von IT-Services sicher und erschliesst unter anderem die Aufgaben des Tagesgeschäfts wie die Bearbeitung von Benutzeranfragen, die Behandlung von Störungen oder die Entwicklung von Problemlösungen. In der Service-Operation-Phase sind das Event Management, Incident Management, Request Fulfillment, Problem Management und Access Management angesiedelt. Ein Event ist ein Ereignis, welches einen unvorhergesehen sowie direkten oder indirekten Einfluss auf ein IT-Service hat und im Event Management überwacht sowie behandelt wird. Neben dem Event existiert der Incident als Begriff, der ungeplante Ausfälle von IT-Services beschreibt und im Incident Management zeitnah sowie effizient gelöst wird. Im Request Fulfillment werden Service Requests, Anfragen von Anwendern wie beispielsweise das Zurücksetzen von Passwörtern, entgegengenommen und abgewickelt. Das Problem Management diagnostiziert die Ursachen eines einzelnen oder mehrerer Incidents und leitet Aktivitäten zur Beseitigung der Ursachen ein. Das Access Management verwaltet den Zugriff von Identitäten auf IT-Services im Hinblick auf die Autorisierung (Steinberg, 2011).

Die Service-Improvement-Phase sichert und überwacht gemäss Lloyd (2011) fortlaufend die Qualität von IT-Services. Die Continual Service-Improvement-Phase identifiziert Verbesserungen für IT-Services, indem sie Daten aus allen Phasen vom Servicelebenszyklus zu den IT-Services sammelt. Zentral für die Continual-Service-Improvement-Phase ist der Seven-Step Improvement Process. Die sieben Schritte sind

1. das Identifizieren einer Verbesserungsstrategie,
2. das Identifizieren der Indikatoren,
3. das Sammeln und Messen der Daten,
4. das Verarbeiten der Daten,
5. das Analysieren der Daten,
6. das Präsentieren und Verwenden der Informationen und
7. das Implementieren der Korrekturmassnahmen (Lloyd, 2011).

2.2 Definition von IT-GRC

Nach Racz, Weippl, & Bonazzi (2011) wurden die Konzepte von Governance, Risk und Compliance erstmalig von PricewaterhouseCoopers (2005) offiziell zusammen und als ein voneinander abhängiges Themengebiet vorgestellt. Governance, Risk und Compliance waren zu diesem Zeitpunkt als einzelne Konzepte nicht neu. In den folgenden Jahren nach der Präsentation von PricewaterhouseCoopers (2005) hat sich das Akronym GRC rasant in verschiedenen Auslegungen ausgebreitet und so zum Beispiel den Weg in Marketingkampagnen oder in Abteilungsnamen von globalen Unternehmen gefunden (Racz et al., 2010, S. 106). Die verschiedenen Definitionen von GRC sind daran zurückzuführen, dass GRC von der Geschäftswelt getrieben wird und hauptsächlich Software-Anbieter, Analysten und Berater in 94% aller publizierten GRC-Artikel einfliessen, welche in einer Studie von Racz et al. (2010, S. 109) ausgewertet wurden.

2.2.1 Abhängigkeit von Governance, Risk und Compliance

Das Akronym GRC findet grosse Beliebtheit in Bezug auf unterschiedliche Themen und damit in unterschiedlicher Auslegung. Hardy und Leonard (2011) haben eine Literaturstudie mit dem Ziel zur Klärung der unterschiedlichen Begrifflichkeit, Definition und Auslegung von GRC durchgeführt. Die in der Literaturstudie gesammelten Betrachtungsweisen von GRC interpretieren die Zusammenführung der Themen Governance, Risk und Compliance entweder erstens als Ansatz, zweitens als System beziehungsweise als Software oder drittens als Projekt zur Verbesserung der Governance durch oder während des Risk Managements und Compliance Managements (Hardy & Leonard, 2011).

Grundsätzlich spricht GRC die Verantwortlichkeiten, die zuverlässige Zielerreichung, die Unsicherheiten und das Handeln mit der Integrität eines Unternehmens an (Hardy & Leonard, 2011). Weiter halten Hardy und Leonard (2011) in ihrer Literaturstudie fest, dass ein integrativer und übergreifender Ansatz zu GRC das Geschäftsergebnis positiv beeinflusst und Geschäftsausfälle minimiert beziehungsweise abschwächt. Racz u. a (2010, S. 113) haben einen Bezugsrahmen für integriertes GRC gemäss der Abbildung 3 eruiert. In den Kernthemen Governance, Risk-Management und Compliance sind die vier Komponenten Strategie, Prozesse, Technologie und Menschen involviert. Daneben wird der Risikoappetit der Organisation zusammen mit den internen und den externen Vorgaben als Regeln definiert. Die drei Kernthemen, die vier Komponenten und die drei Regeln werden zusammengeführt und auf die Geschäftstätigkeiten ausgerichtet. Gemäss der Abbildung 3 verbessern die Steuerung und Unterstützung der Geschäftstätigkeiten durch GRC das

ethische Verhalten, die Effizienz und die Effektivität. Die drei Hauptmerkmale des Bezugsrahmen von Racz u. a (2010, S. 113) sind, dass integriert, ganzheitlich und organisationsweit vorgegangen wird.

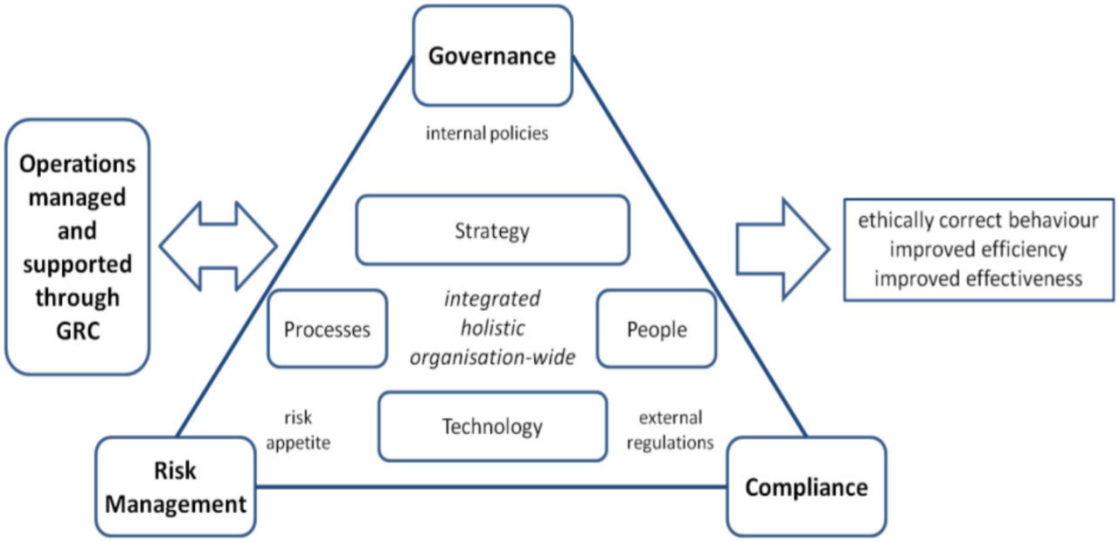


Abbildung 3: Bezugsrahmen für integriertes GRC (Racz et al., 2010, S. 113)

Im Grundsatz werden Unternehmen durch integriertes GRC bei der Erfüllung von aufsichtsrelevanten Anforderungen unterstützt (Moeller, 2013, S. 44). Transformationen von Geschäftsprozessen werden erleichtert, tiefere Einblicke in die Geschäftsprozesse ermöglicht und genauere Prognosen anhand der Geschäftsinformationen getroffen (Moeller, 2013, S. 44). Zu den wichtigsten Faktoren zur Ausübung von GRC gehören die Fähigkeiten, Informationsbestände besser zu verwalten, die Einhaltung gesetzlicher und regulatorischer Verpflichtungen nachzuweisen, allfällige Risiken und die damit verbundenen Kosten zu verringern, die Kosten zur Nutzung von Informationen für Audits zu senken und die Verantwortlichkeit des Unternehmens zu belegen (Moeller, 2013, S. 44).

2.2.2 Bezug der IT zu GRC

Auch in IT-Organisationen ist GRC immer öfters anzutreffen, da mit der gleichzeitigen Ausbreitung der Digitalisierung von Geschäftsprozessen und der steigenden Komplexität auch die Nachfrage an IT-orientiertem GRC steigt. Die hohe Dynamik der IT konfrontiert Unternehmen mit zwei Konsequenzen (Marekfia & Nissen, 2009, S. 2). Einerseits müssen Unternehmen die GRC-Aktivitäten aufgrund der hohen Dynamik ausweiten (Marekfia & Nissen, 2009, S. 2). Andererseits besteht der Druck, die Kerngeschäftsprozesse flexibel zu halten, um rechtzeitig auf Marktveränderungen reagieren zu können (Marekfia & Nissen, 2009, S. 2). Grosse Unternehmen setzen die IT nicht nur zur Unterstützung des Geschäfts, sondern teilweise auch als Business Enabler und Innovator ein, um überhaupt Geschäftstätigkeiten zu ermöglichen (Albayrak & Gadatsch, 2017, S. 154). Da GRC generell ein ganzes Unternehmen und damit auch die IT umfasst, kann nach Marekfia und Nissen (2009, S. 2) deren Vernachlässigung zu ökonomisch gravierenden Nachwirkungen führen. Aus dem beidseitigen Interesse an die IT und an GRC hat sich der Begriff IT-GRC entwickelt, welcher sich vom Corporate GRC abgrenzt. Für IT-GRC ist gemäss der Abbildung 4 die IT-Organisation der Dreh- und Angelpunkt, wo hingegen für das Corporate GRC das ganze Unternehmen zentral ist. IT-GRC fungiert zwischen dem unternehmensübergreifendem GRC und der IT, bei welcher unter anderem mit der Governance eine IT-Organisation an die Unternehmensziele ausgerichtet, mit dem Risk-Management mögliche Gefahren behandelt und mit der Compliance die Vorgabeneinhaltung gesichert werden sollen. In den folgenden Unterkapiteln wird der Bezug der IT zu Governance, Risk und Compliance ausgelegt.

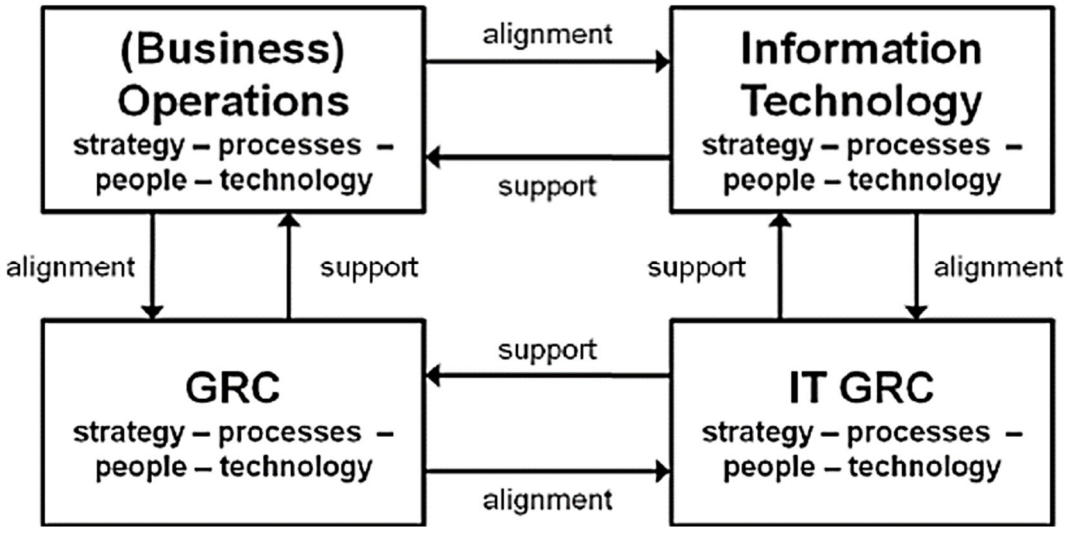


Abbildung 4: Kontext von GRC und IT-GRC (Racz et al., 2010, S. 114)

2.2.2.1 IT-Governance

Unter Governance wird die verantwortliche, transparente und nachvollziehbare Leitung und Kontrolle eines Unternehmens durch ein Governance Body oder, auf Deutsch, durch ein Leitungsorgan verstanden (Knoll & Strahringer, 2017, S. 2). Governance nicht nur auf das gesamte Unternehmen ausgelegt, sondern kann sich durch Governance Bodies auch auf Einheiten, Abteilungen oder materielle beziehungsweise immaterielle Vermögenswerte beziehen (ISACA, 2012). Das IT-Risk Acceptance Board, welches über die Frage der Risikoakzeptanz entscheidet, ist ein Beispiel eines Governance Body, welches in Form von Gremien aufgebaut ist (Knoll & Strahringer, 2017, S. 9 f.). Im Zusammenhang mit Governance tauchen die zwei Begriffe Corporate Governance und IT-Governance auf. Urbach und Gschwendtner (2012, S. 5) unterordnen IT-Governance als einen Bestandteil der Corporate Governance. Nach Knoll & Strahringer (2017, S. 2) schliesst Corporate Governance alle Prozesse des Unternehmens zur Sicherstellung einer verantwortungsvollen Unternehmensführung und -kontrolle ein. Weiter beeinflusst Corporate Governance nach Knoll und Strahringer (2017, S. 2) IT-Governance aufgrund der stetig an Bedeutung gewinnenden IT-Prozesse, da der Fokus von IT-Governance auf der IT-Organisation und damit auch auf den IT-Prozessen liegt.

IT-Governance besteht gemäss der Abbildung 5 aus den drei Schritten der Evaluierung, Leitung und Überwachung von IT-Organisationen. In einem ersten Schritt verlangt die Evaluierung, dass vom Management geschäftskritische Informationen dem Governance Body zeitnah und unverfälscht zur Verfügung gestellt werden, um daraus den aktuellen und den zukünftigen Nutzen der IT zu bestimmen (Mayer, Barafort, Picard, & Cortina, 2015, S. 90). Neben den geschäftskritischen Informationen fliessen die Pläne und die Vorschläge des Managements wie auch die Verbesserungen der eigenen Überwachung gemäss der Abbildung 5 mit ein. In einem zweiten Schritt legt der Governance Body aus den Erkenntnissen der Evaluierung die Strategien und Richtlinien fest. Für die Entscheidungsfindung der Strategien und Richtlinien bezieht der Governance Body die Anforderungen möglichst aller Anspruchsgruppen mit ein (Racz, Weippl, & Seufert, 2010 in Govindji, Peko, & Sundaram, 2018, S. 15). Ein Beispiel für eine Anforderung an IT-Governance ist die Sicherstellung, dass die Strategie der IT-Organisation jener des Unternehmens entspricht. Das operative Management ist der IT-Governance unterstellt und setzt die vom Governance Body beschlossenen Strategien und Richtlinien um. Durch die Strategien und Richtlinien bildet IT-Governance für das Management die Grundlage, der Situation entsprechende Managemententscheidungen zu treffen.

Diese Managemententscheidungen betreffen Grundsätze, Verfahren und Massnahmen unter anderem zur Erreichung der Unternehmensziele, zum verantwortungsvollen Einsatz der Ressourcen oder zur angemessenen Überwachung von Risiken (Knoll & Strahringer, 2017, S. 3). Die ISO/IEC 38500 definiert das Management als ein aus Prozessen und Kontrollen bestehendes System, welches das Erreichen der strategischen Ziele beabsichtigt (Johannsen & Goeken, 2011). In einem dritten Schritt werden die Leistung und Konformität unter Bezugnahme auf die Abbildung 5 überwacht, woraus wiederum Verbesserungen bei Abweichungen für die Evaluierung einfliessen. Der zentrale Nutzen von IT-Governance ist die Steuerbarkeit der IT, was nach Urbach und Gschwendtner (2012, S. 28) zu einer Erhöhung der Kosten- und Serviceeffizienz der IT, der Effektivität der IT, der Minderung von IT-Risiken und der Verbesserung der IT-Compliance führt.

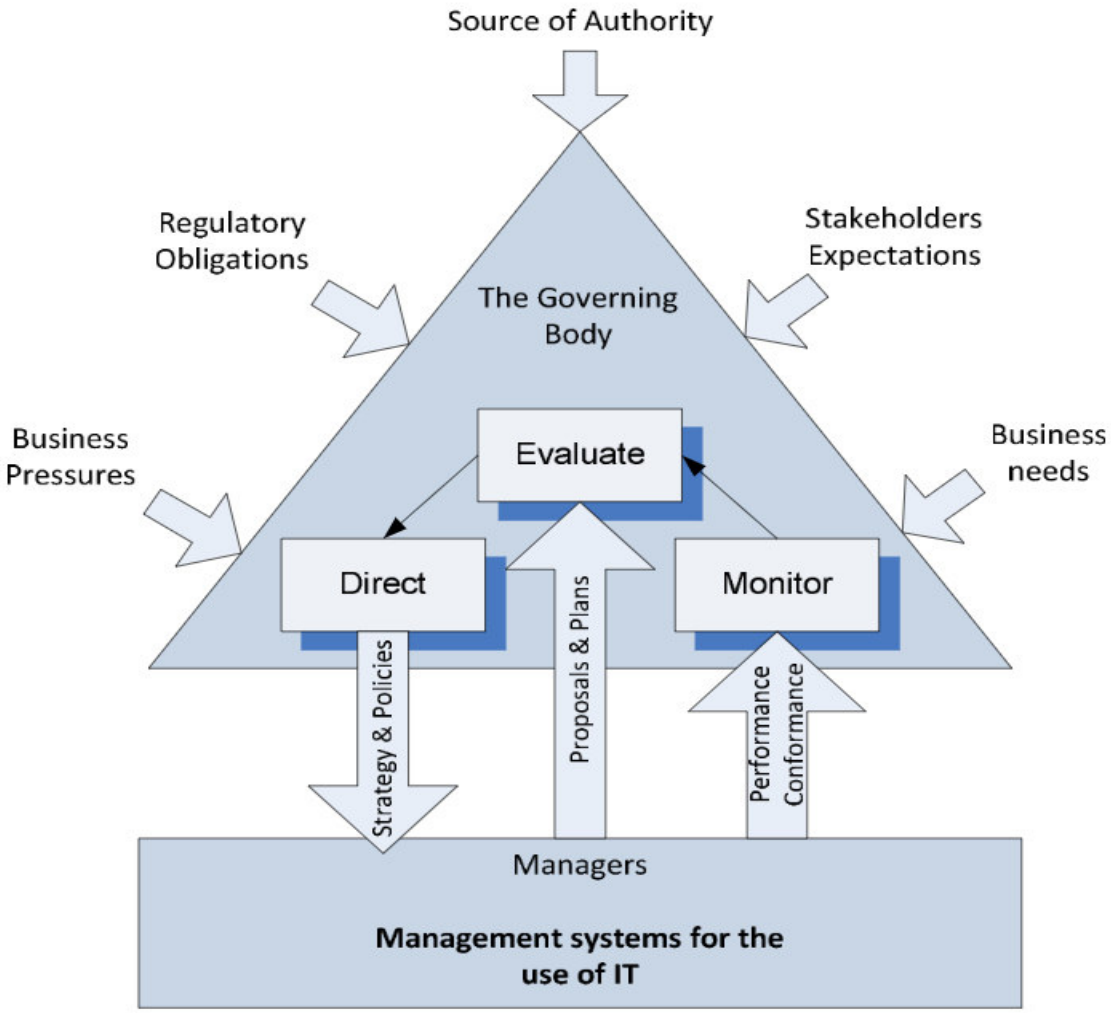


Abbildung 5: Modell für IT-Governance (Mayer et al., 2015, S. 91)

2.2.2.2 IT-Risk

Disterer (2017, S. 84) definiert Risk oder auch Risiko im Grundsatz als die theoretische Möglichkeit, in Zukunft einen Schaden zu erleiden. Risiken, die mit Schaden in Relation stehen, werden auch als Gefahren bezeichnet. Weniger in Erscheinung treten positive Risiken, die sich für das Unternehmen als Chancen anbieten. Sowohl nach Kraft und Stöwer (2017, S. 99) als auch nach Knoll und Strahringer (2017, S. 3) ändern sich mit der Digitalisierung von Geschäftsprozessen zeitgleich die Risiken eines Unternehmens. Als IT-Risiken werden jene Gefahren bezeichnet, die aus dem Betrieb und der Nutzung der IT entstehen (Disterer, 2017, S. 84). Die IT-Risiken müssen in einem Risk-Management beherrscht werden und sollten gemäss Knoll und Strahringer (Knoll & Strahringer, 2017, S. 19) nicht nur wie in der Regel einmal im Jahr gehandhabt, sondern aufgrund der zunehmenden Digitalisierung und damit der zunehmenden Veränderungen häufiger geprüft werden. Durch die Veränderungen im Unternehmen, in der IT selbst und im Umfeld können neue Risiken entstehen oder bestehende Risiken sowohl negativ als auch positiv beeinflusst werden (Knoll & Strahringer, 2017, S. 19). Aufgrund der Komplexität und der Vielfältigkeit der IT sind nach Knoll und Strahringer (2017, S. 21) IT-Risiken oftmals aufwändiger zu erkennen und zu umgehen. Die Geschäftsleitung verantwortet einen allfälligen Schaden gegen aussen, wobei nach innen die Verantwortungen klar zu regeln sind (Knoll & Strahringer, 2017, S. 10). Gemäss der Experteninterviews ist der Hauptverantwortliche einer IT-Organisation der CIO. Die Regelung der Verantwortlichkeiten stützt sich auf das Prinzip der Festlegung von Risk-Ownern, welche intern die Verantwortung für Risiken tragen, und Risk-Managern, welche die Aktivitäten koordinieren und an den die Risk-Owner berichten (Knoll & Strahringer, 2017, S. 10). Für die Zuteilungen der internen Verantwortlichkeiten müssen auch die Lieferanten als Risikopotenziale miteinbezogen werden (Knoll & Strahringer, 2017, S. 10). Für IT-Organisationen zählen zum Beispiel Anbieter von Outsourcing- oder Cloud-Lösungen zu den Lieferanten.

Die zentralen Prozesse des Risk-Managements sind nach Knoll und Strahringer (2017, S. 14 ff.) die fünf Schritte der Kontextdefinition, der Identifikation, der Analyse, der Bewertung und der Behandlung von Risiken (vgl. Abbildung 6). Im ersten Schritt wird der Kontext festgelegt. Im Kontext werden die Ziele der Organisation zum Risk-Management dargestellt, die Bedürfnisse aller Anspruchsgruppen berücksichtigt und die Kriterien für Risiken definiert. Im zweiten Schritt werden die IT-Risiken eines Unternehmens identifiziert. Kraft und Stöwer (2017, S. 105) nennen jene IT-Risiken als Beispiele, die hohe Verluste bei Störungen oder Ausfällen von Anwendungssystemen, IT-Infrastruktur oder

IT-Prozessen verzeichnen oder wo die Vertraulichkeit sensibler Daten, die gesetzlichen Auflagen oder andere externe Verpflichtungen verletzt werden können. Die Herausforderung in der Identifikation der Risiken liegt darin, keine Risiken zu übersehen. Im dritten Schritt werden alle identifizierten Risiken analysiert. Die Eintrittswahrscheinlichkeit und des Schadensausmasses jedes einzelnen Risikos werden gegenübergestellt. Kraft und Stöwer (2017, S. 106) stellen fest, dass das Abbilden von Risiken in Matrizen mit niedrigen, mittleren und hohen Einstufungen eine hohe Beliebtheit im Risk-Management geniesst. Im vierten Schritt werden die Risiken bewertet. In der Bewertung werden die Folgen des Unternehmens bei einem Eintritt und damit die Priorität der Behandlung des Risikos bestimmt. Im fünften Schritt werden die Risiken behandelt. Die Behandlung der Risiken umfasst die Möglichkeiten zur grösstmöglichen Vermeidung, zur Verringerung der Eintrittswahrscheinlichkeit und des Schadensausmasses, zur Transferierung an Partner oder Versicherungen und notfalls zur Akzeptierung der verbliebenen Risiken (Knoll & Strahringer, 2017, S. 18). Die fünf zentralen Prozesse des Risk-Management sind in der Abbildung 6 dargestellt. Sie werden laufend überwacht und durch das Risikoberichtswesen, die Kommunikation und die Beratung, die IT-Risikosteuerung und durch die fortlaufende Verbesserung begleitet (Knoll & Strahringer, 2017, S. 18 f.).

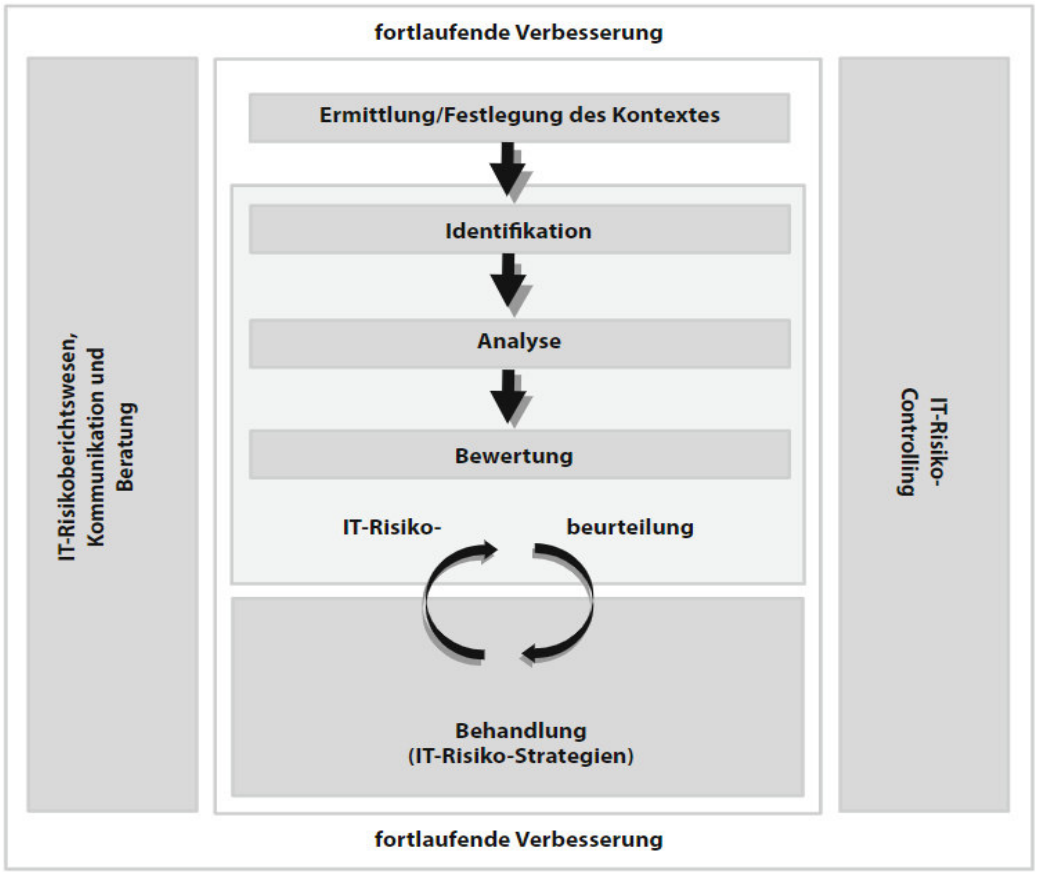


Abbildung 6: IT-Risikomanagemenet-Prozess (Knoll, 2017, S. 13)

2.2.2.3 IT-Compliance

Durch Unternehmensskandale wie dem Abgasskandal verschiedener Autohersteller im Jahr 2015 oder dem schweren Korruptionsfall von Siemens im Jahr 2006, wo laut Feldges (2018) zusätzlich zu einer Milliardenbusse auch eine langjährige Aufarbeitung des grössten deutschen Industriekonzerns nötig war, stieg in der Geschäftsführung vieler Unternehmen die Nachfrage an verbesserter Transparenz. In der Studie von Urbach und Gschwendtner (2012, S. 22) streben 64% der Studienteilnehmer nach einer Erhöhung der Transparenz. Infolgedessen verpflichten sich Unternehmen laut Knoll und Strahringer (2017, S. 5), interne sowie externe Vorgaben in einem ersten Schritt zu erkennen und in einem zweiten Schritt zu prüfen, um damit Compliance oder auf Deutsch Konformität zu erwirken. Die Einhaltung von Compliance umfasst ganze Unternehmen, wobei IT-Compliance direkten oder indirekten Einfluss auf IT-Organisationen ausübt und in drei Stufen unterteilt werden kann (Knoll & Strahringer, 2017, S. 6). Die erste und grundlegendste Stufe verlangt, gesetzliche Vorgaben einzuhalten und zu überwachen. Zwei Beispiele für gesetzliche Vorgaben sind die GDPR und der Sarbanes-Oxley Act (SOX). Die zweite Stufe beinhaltet die Implementation von Industriestandards oder Normen wie beispielsweise der ISO/IEC-27000. Die oberste und dritte Stufe beinhaltet freiwillige Vorgaben. Ein Beispiel dieser dritten Stufe ist das Engagement, die Prozesse der IT-Organisation an den Best-Practice-Ansätzen von ITIL V3 2011 auszurichten.

Oftmals bestehen Differenzen zwischen den Zielen der Compliance und den Zielen des operativen Geschäfts (Schneider, 2018, S. 45). Um die Differenzen im Interesse des Unternehmens anzugehen, wird meistens ein Internes Kontrollsystem (IKS) als Überwachungsinstrument eingesetzt. Ein IKS schliesst Kontrollmechanismen sowohl in detektiver als auch in präventiver Form ein (Hunziker, Renggli, & Fallegger, 2018b, S. 4). Seit dem Jahr 2008 müssen Unternehmen in der Schweiz ein IKS nachweisen (Hunziker, Renggli, & Fallegger, 2018a, S. 1). Analog zu IT-Risiken trägt die Geschäftsleitung nach aussen die Verantwortung der IT-Compliance. Ein IT-Compliance-Officer steuert und verantwortet die IT-Compliance-Aktivitäten nach innen, dient dem Chief Compliance Officer (CCO) oder dem Chief Information Officer (CIO) als Stabsstelle und führt IT-Compliance-Beauftragte, welche die Compliance-Aktivitäten der jeweiligen Abteilungen ausführen. IT-Organisationen profitieren von IT-Compliance, indem der Wertbeitrag sowie die Sicherheit der IT steigt und allfällige Kosten für Schadenersatzzahlungen, Strafen oder Reputationsschäden gemindert werden (Knoll & Strahringer, 2017, S. 20).

2.2.3 COBIT 5 als Framework für IT-GRC

Für das Anwendungsgebiet von IT-GRC bietet sich COBIT 5 als Framework an (Andelfinger & Kneuper, 2017, S. 27). In der Zwischenzeit hat ISACA (2018) die neuere Version COBIT 2019 veröffentlicht, welche den Begriff *Enterprise Governance of Information and Technology* (EGIT) für eine höhere Akzeptanz und Umsetzbarkeit in Unternehmen in den Fokus setzt. Da die ITSM Lösungsanbieter sich erst in COBIT 2019 einarbeiten und anpassen müssen, dient COBIT 5 als theoretische Grundlage der Bachelorarbeit. Gemäss ISACA (2012) verfolgt COBIT 5 auf Basis der durchgängigen Anwendung von fünf grundlegenden Prinzipien und der Berücksichtigung von sieben Enabler die Ziele von effektivem IT-Business-Alignment, Governance und Compliance. Die fünf Prinzipen setzen sich aus der Erfüllung der Anforderungen der Anspruchsgruppen, der Abdeckung des gesamten Unternehmens, der Anwendung eines einheitlichen, integrierten Frameworks, der Ermöglichung eines ganzheitlichen Ansatzes und dem Unterscheiden zwischen Governance und Management zusammen (ISACA, 2012). Die sieben Enabler werden von COBIT 5 als kritische Erfolgsfaktoren zur Erreichung der IT-Ziele genannt und beinhalten erstens Prinzipien, Richtlinien und Rahmenwerke, zweitens Prozesse, drittens Organisationsstrukturen, viertens Kultur, Ethik und Verhalten, fünftens Informationen, sechstens Services, Infrastruktur und Anwendungen und siebtens Mitarbeiter, Fähigkeiten und Kompetenzen (ISACA, 2012). COBIT 5 unterteilt insgesamt 37 Governance- und Managementprozesse in zwei Hauptbereiche (vgl. Abbildung 7).

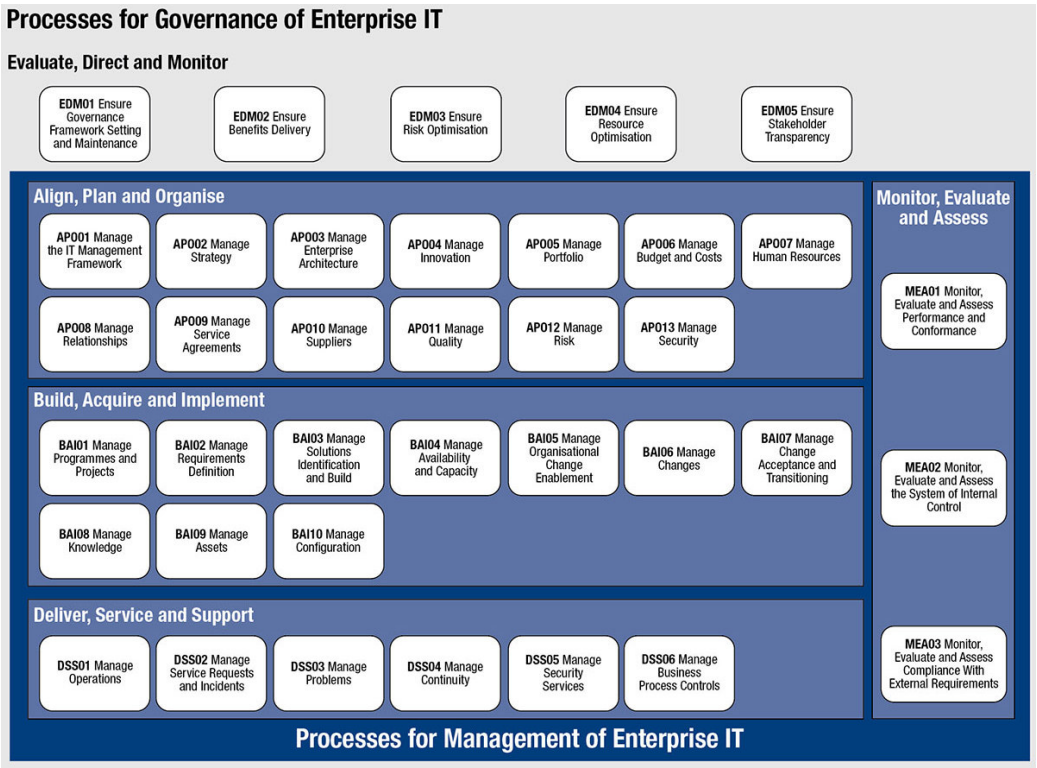


Abbildung 7: COBIT 5 Prozess Referenzmodell (ISACA, 2012)

Der erste Hauptbereich von COBIT 5 umfasst fünf Governance-Prozesse, in der Praktiken zur Evaluierung, Leitung und Überwachung der IT-Organisation definiert werden (ISACA, 2012). Die Evaluierung, Leitung und Überwachung der IT-Organisation bilden auch in COBIT 5 die Basis der Governance, welche die Einrichtung und Pflege eines Governance-Rahmenwerks, die Lieferung von Wertbeiträgen, die Risikooptimierung, die Ressourcenoptimierung und die Transparenz gegenüber Anspruchsgruppen sicherstellt. Der zweite Hauptbereich von COBIT 5 umfasst Managementprozesse, die in vier weitere Bereiche aufgeteilt sind und auf Basis von Plan, Build, Run and Monitor eine durchgängige Abdeckung des IT-Managements sicherstellen (ISACA, 2012).

IT-Risk wird von COBIT 5 sowohl in einem Prozess der IT-Governance als auch in einem Prozess des IT-Managements gemäss der Abbildung 7 direkt behandelt. In der Governance überschneidet sich IT-Risk zum einen mit dem Prozess EDM03 gemäss der Abbildung 7, welcher die Sicherstellung der Risikooptimierung anvisiert. Die Sicherstellung der Risikooptimierung beinhaltet die Identifizierung aller IT-bezogenen Risiken und das Verständnis des Risikoappetits von Unternehmen. COBIT 5 definiert als Ziel vom Prozess EDM03, dass die IT-Risiken identifiziert und der Risikoappetit kommuniziert, dass kritische IT-Risiken effektiv verwaltet und dass IT-Risiken innerhalb des Risikoappetits gehalten werden. Der Prozess EDM03 steht in Relation mit vier Zielen der IT, indem Einfluss auf die Verwaltung von IT-bezogenen Geschäftsrisiken, auf die Transparenz von Kosten, Nutzen und Risiken der IT, auf die Sicherheit von Informationen, Verarbeitungsinfrastruktur und Applikationen sowie auf die Sicherstellung der IT-Compliance von internen Vorgaben Einfluss ausgeübt wird (ISACA, 2012).

Im Management beziehungsweise im Bereich Anpassen, Planen und Organisieren ist der Prozess APO12 gemäss der Abbildung 7 für IT-Risk relevant. Der Prozess APO12 identifiziert, beurteilt und verwaltet Risiken, pflegt ein vollständiges Risikoprofil, verwaltet die Risk Management Aktivitäten und gewährleistet die effektive Implementierung von Risk Management Aktivitäten. Weiter erstrebt der Prozess APO12 die Integration vom IT-Risk-Management mit dem Enterprise-Risk-Management. Der Prozess APO12 steht in Relation mit fünf Zielen der IT zur Sicherstellung der IT-Compliance von externen Vorgaben, der Verwaltung von IT-bezogenen Geschäftsrisiken, der Transparenz von Kosten und Nutzen der IT, der Sicherheit von Informationen und Applikationen sowie der termin- und budgetgerechten Lieferung von Programmen (ISACA, 2012).

IT-Compliance wird von COBIT 5 im Prozess MEA03 gemäss der Abbildung 7 direkt behandelt, welcher im Management beziehungsweise im Bereich Überwachen, Evaluieren und Beurteilen angesiedelt ist. Konkret überwacht, evaluiert und beurteilt der Prozess MEA03 die IT-Compliance mit externen Anforderungen, indem alle externen Vorgaben identifiziert und die externen Vorgaben angemessen adressiert werden. Der Prozess MEA03 betrifft die zwei Ziele der IT, dass die IT-Compliance und Unterstützung für Business Compliance mit externen Vorgaben sowie dass die Verwaltung von IT-bezogenen Geschäftsrisiken sicherzustellen sind (ISACA, 2012).

2.3 Berührungspunkte von ITSM und IT-GRC

Sowohl dem ITSM als auch dem IT-GRC steht ein zentraler Stellenwert aus Sicht von IT-Organisationen zu. Als weltweit etabliertes Framework dient ITIL V3 2011 wie in Kapitel 2.1.2 beschrieben für die Auslegung von ITSM, wobei gemäss Kapitel 2.2.2 die Aufgaben von IT-GRC in COBIT 5 beschrieben werden. In diesem Kapitel werden zuerst die beiden Frameworks ITIL V3 2011 und COBIT 5 gegenübergestellt. Im zweiten Unterkapitel folgt die Zuordnung von ITSM und IT-GRC.

2.3.1 Gegenüberstellung von ITIL V3 2011 und COBIT 5

Die IT-Services und die Art, wie die IT-Services verwaltet werden, bilden den Dreh- und Angelpunkt von ITIL V3 2011 (Teubner & Remfert, 2017, S. 451). Das Ziel von ITIL V3 2011 ist, die IT-Organisation stärker an das Kerngeschäft des Kunden zu binden, indem die IT-Services nach den Bedürfnissen der Kunden ausgerichtet und das Verständnis sowie die Interaktion zwischen der IT-Organisation und dem Kunden gefördert werden (Teubner & Remfert, 2017, S. 454). ISACA (2012, S. 15) nennt als zentralen Ausgangspunkt für IT-Organisationen, dass sowohl die Abhängigkeit zwischen dem Erfolg und der externen Geschäftspartner als auch die Menge an Informationen deutlich zunehmen. COBIT 5 liefert Ansätze, wie Anspruchsgruppen bei der Entscheidungsfindung einzubeziehen und wie Entscheidungen im Sinne der strategischen Ziele sowie der Compliance zu treffen sind (ISACA, 2012). Weiter werden Lösungsansätze von COBIT 5 geboten, wie mit einer weitaus umfassenderen IT umzugehen ist, die immer mehr zu einem integralen Bestandteil des Unternehmens wird (ISACA, 2012). Eine effektive IT-Governance ermöglicht wirtschaftliche Vorteile und minimiert Risiken der IT-Organisation. Zwischen der Umsetzung von ITIL V3 2011 und der Umsetzung von COBIT 5 besteht ein enger Zusammenhang, da nach Percheiro et al. (2017, S. 480) beide Frameworks IT-Organisationen dabei unterstützen, die Bestrebungen nach höherer Effizienz und Effektivität zu

meistern. ITIL V3 2011 und COBIT 5 stehen komplementär zueinander, da gemäss der Experteninterviews und nach Glenfis AG (o. J.) Prozesse aus ITIL V3 2011 und aus COBIT 5 sich decken und ergänzen.

Beim Vergleich von ITIL V3 2011 und COBIT 5 zeigt sich, dass ITIL V3 2011 sich eher auf die operative Sicht auf IT-Organisationen und COBIT 5 sich eher auf die strategische Sicht auf IT-Organisationen fokussiert. Auf der einen Seite wird die von ITIL V3 2011 operativere Sicht auf IT-Organisationen dadurch begründet, dass der Fokus gemäss der Experteninterviews in der betrieblichen Optimierung liegt, wie IT-Services über den gesamten Servicelebenszyklus verwaltet werden. Auf der anderen Seite lässt sich die von COBIT 5 strategischere Sicht auf IT-Organisationen darauf zurückführen, dass gemäss der Experteninterviews die Steuerung, Kontrolle oder Assessments von IT-Organisationen eine Ausprägung von COBIT 5 ist. Nach Ableitung der Experteninterviews sind hauptsächlich in der Service Strategy sowie im Service Design Überschneidungen ausfindig zu machen. Umgekehrt deckt ITIL V3 2011 in COBIT 5 die Managementprozesse der Bereiche *Anpassen, Planen und Organisieren*, *Aufbauen, Beschaffen und Implementieren* sowie *Bereitstellen, Betreiben und Unterstützen* (vgl. Abbildung 8).

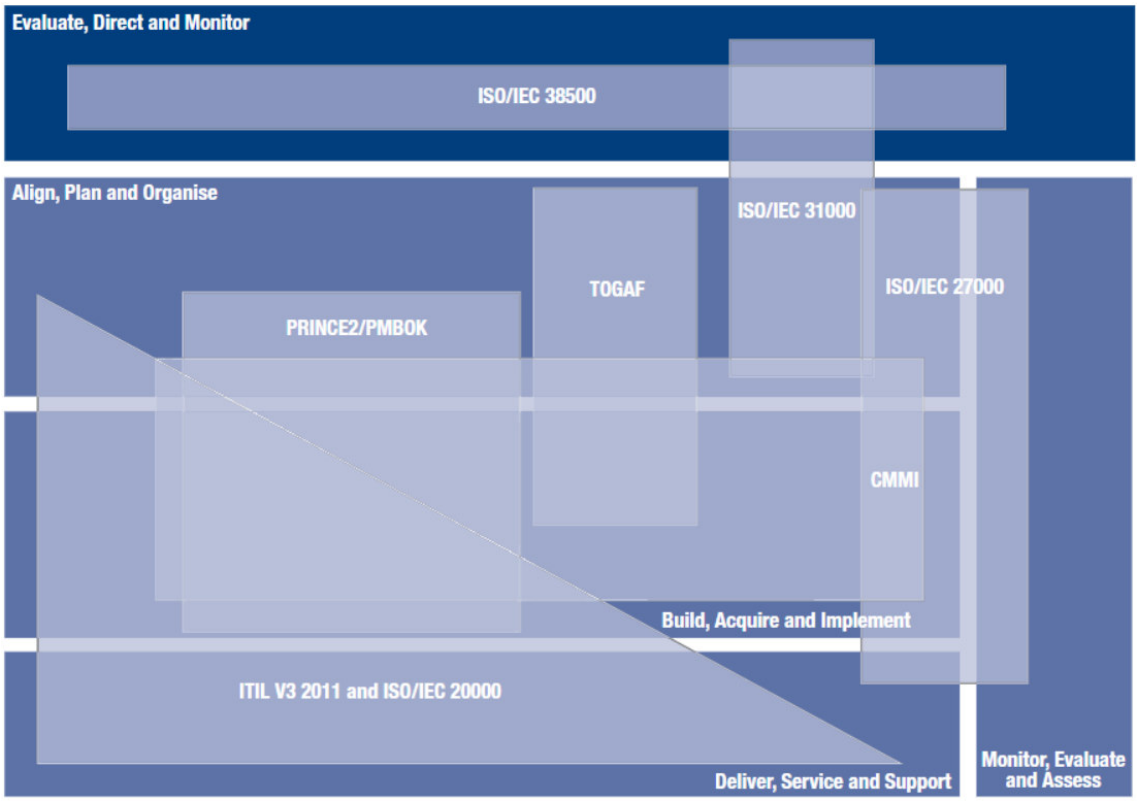


Abbildung 8: COBIT 5 Abdeckung von ITIL V3 2011 (ISACA, 2012)

2.3.2 Zuordnung von ITSM und IT-GRC

IT-Services ermöglichen die Ausführung von Geschäftsprozessen, indem beispielsweise den Benutzern Softwarefunktionalitäten zur Verfügung gestellt und damit Hardware sowie Software als Potenzialfaktoren genutzt werden (Teubner & Remfert, 2017, S. 451). Da die IT-Services nach Teubner und Remfert (2017, S. 451) von Potenzialfaktoren gebildet werden, der Output von IT-Organisationen auskommt und das ITSM die IT-Services und damit deren Potenzialfaktoren steuert, besteht die Notwendigkeit für die Ausübung von IT-GRC auf ITSM. ITSM fungiert somit als Gegenstand beziehungsweise als Bewertungsobjekt von IT-GRC, um anhand von IT-GRC gemäss der Abbildung 9 das ethische Verhalten, die Effizienz und die Effektivität von ITSM zu verbessern.

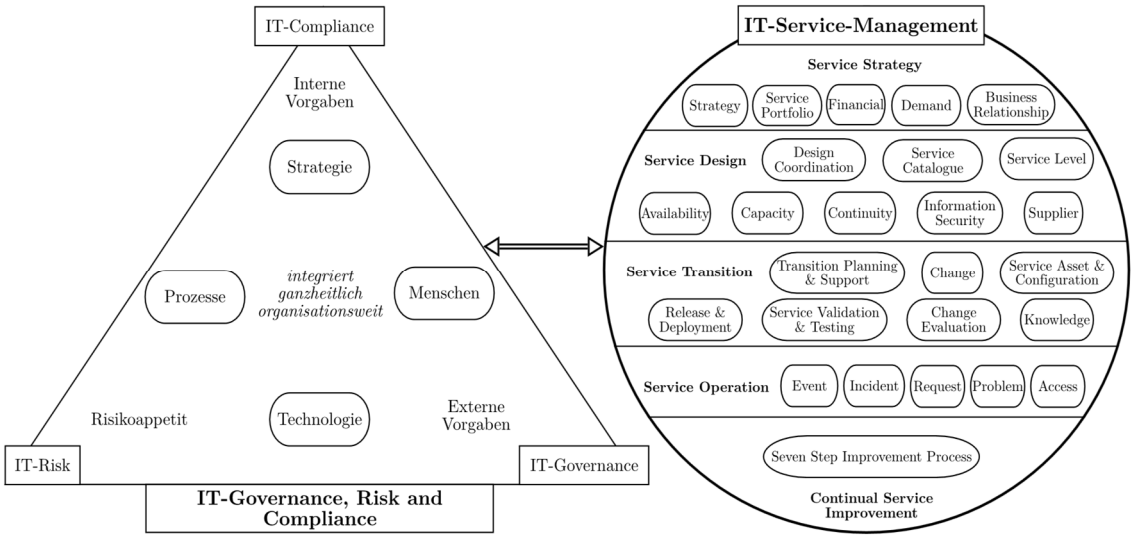


Abbildung 9: ITSM als Bewertungsobjekt von IT-GRC

Nach Marekfia und Nissen (2009, S. 2) fördert das ITSM die Ausübung von IT-GRC aufgrund der zunehmenden Kundenorientierung von IT-Organisationen. Die damit verbundene, steigende Komplexität von Risiken und Vorgaben aufgrund der sich gemäss Pröhl und Zarnekow (2019) stetig verändernden Kundenbedürfnisse unterstreichen die Nachfrage an der Ausübung von IT-GRC in Bezug auf ITSM. Neben IT-GRC von ITSM besteht die Möglichkeit, IT-GRC in das ITSM der IT-Organisation zu integrieren und IT-GRC durch das ITSM auszuüben, indem ITSM als Werkzeug genutzt wird. Mit der Ausübung von IT-GRC durch das ITSM profitiert gemäss der Experteninterviews ein Unternehmen von der Möglichkeit, die zwei Welten von IT-GRC und ITSM miteinander zu verbinden. Sowohl die Qualität als auch die Geschwindigkeit können gemäss der Experteninterviews optimiert werden, da aufgrund einer Integration von IT-GRC in ITSM unter anderem ermöglicht wird, IT-GRC Aufgaben zu automatisieren, mit Objekten aus ITSM

Prozessen zu verknüpfen und diese der Bearbeitung zuzuführen. Führende ITSM Lösungsanbieter erkennen die Potenziale der Einbindung von IT-GRC in ITSM und integrieren IT-GRC als einen eigenen Bereich in ihren ITSM Lösungen. Konkret werden im IT-GRC Bereich der ITSM Lösungen unterschiedliche Funktionen angeboten, welche IT-GRC Aufgaben automatisieren. Beispiele für ITSM Lösungsanbieter, die IT-GRC in ihren ITSM Lösungen integriert haben und in diesem Zusammenhang IT-GRC Funktionen vermarkten, sind unter anderem BMC Software, Cherwell Software oder ServiceNow (BMC Software, 2019; Cherwell Software, 2019a; ServiceNow, 2019b).

Da sich gemäss der Experteninterviews die Auslegung und das Verständnis von IT-GRC durch ITSM je nach ITSM Lösungsanbieter unterscheiden, nur einzelne Bestandteile mit der Bezeichnung IT-GRC von ITSM Lösungsanbietern ausgeliefert werden und damit die IT-GRC Funktionen je nach ITSM Lösung variieren, ist die Auslegung von IT-GRC durch ITSM zu differenzieren. In einem ersten Schritt sind die Aufgaben von IT-GRC zu erörtern, die durch ITSM automatisiert werden können. In einem zweiten Schritt wird aufgezeigt, wie diese Aufgaben mit einem ITSM korrelieren. Abschliessend wird die Nutzung von IT-GRC durch ITSM in einem Venn-Diagramm visualisiert.

2.3.2.1 Auslegung der automatisierbaren IT-GRC Aufgaben

Ein Risk Management und ein Compliance Management bilden gemäss der Experteninterviews die grundlegenden Aufgaben von IT-GRC, welche automatisiert werden können. Das Risk Management umfasst gemäss Mayer et al. (2015, S. 95) Aufgaben, welche Governance Bodies bei der Evaluierung, Leitung und Überwachung der IT-Organisation Unterstützung bieten und in Relation mit Risiken stehen. Im Bereich der Evaluierung trägt gemäss der Abbildung 10 das Risk Management zur Verwaltung von Risikopraktiken bei. Die Risikopraktiken halten fest, wie Risiken zu behandeln sind. Weiter dient der Governance eine Bewertung von Risiken, um besonders die kritischen Risiken früh zu erkennen. Im Bereich der Leitung unterstützt gemäss der Abbildung 10 das Risk Management die Governance Bodies bei der Definition des Risikoappetits. Im Bereich der Überwachung stellt gemäss der Abbildung 10 das Risk Management das Monitoring der Risiken und die Auditabdeckung sicher (Mayer et al., 2015, S. 95).

Analog zum Risk Management unterstützen auch die Aufgaben des Compliance Managements gemäss Mayer et al. (2015, S. 95), welche in Relation mit internen und externen Vorgaben stehen, Governance Bodies bei der Leitung, Evaluierung und Überwachung der IT-Organisation bei. Im Bereich der Evaluierung schafft das Compliance Management gemäss der Abbildung 10 Abhilfe für die Governance bei Überprüfungen der Vorgabenverwaltung. Im Bereich der Leitung werden gemäss der Abbildung 10 zum einen die internen Vorgaben und zum anderen die externen Vorgaben erfasst. Weiter zählt die Regelung der Verantwortlichkeiten zu den Aufgaben, die über das Compliance Management ausgeführt werden. Im Bereich der Überwachung wird gemäss der Abbildung 10 über das Compliance Management die Performance und die Berichterstattung kontrolliert und Compliance Probleme behandelt (Mayer et al., 2015, S. 95).

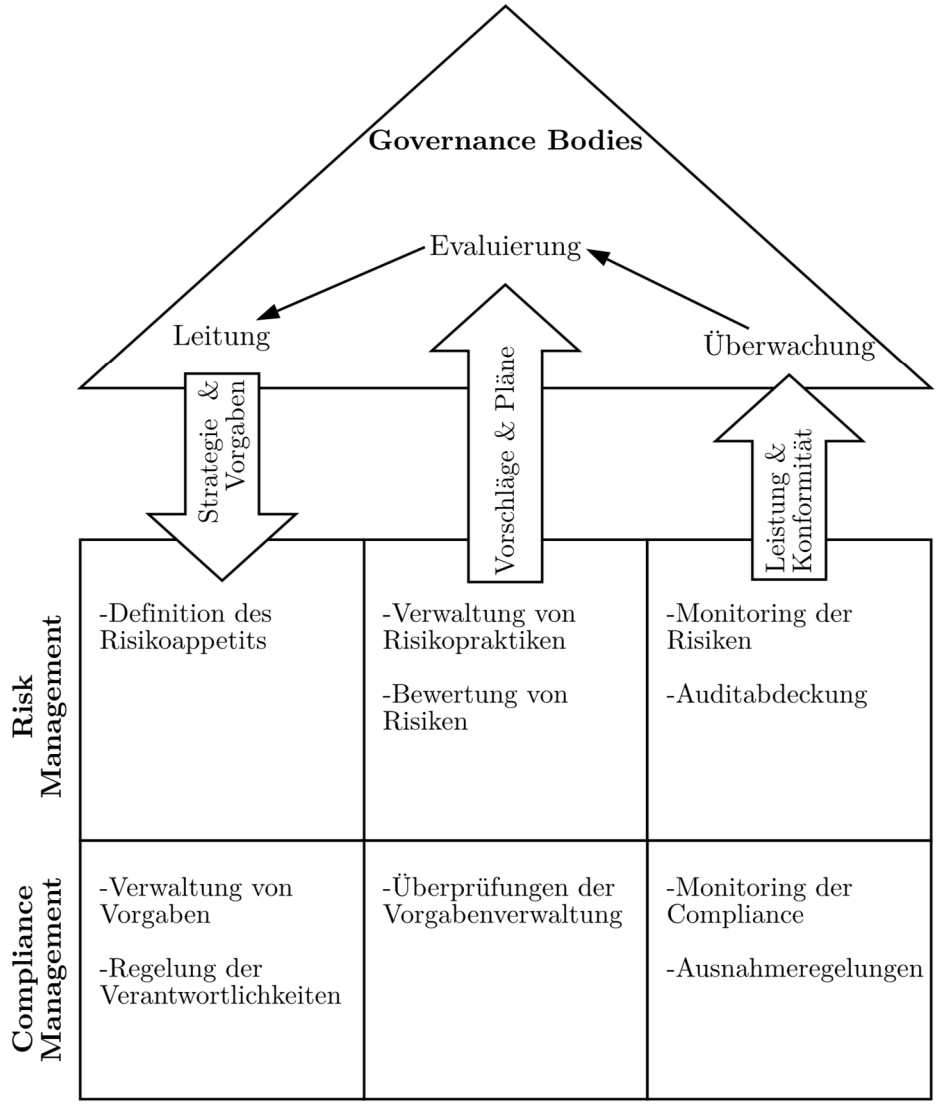


Abbildung 10: IT-GRC Aufgaben in Anlehnung an Mayer et al. (2015, S. 95)

2.3.2.2 Automatisierbare IT-GRC Aufgaben durch ITSM

Die IT-GRC Aufgaben vom Kapitel 2.3.2.1 können gemäss der Experteninterviews über IT-GRC Funktionen automatisiert und gemäss der Abbildung 11 durch ITSM ausgeführt werden. Da ITIL V3 2011 als Framework für ITSM dient, werden die IT-GRC Aufgaben den fünf Phasen des Servicelebenszyklus zugeordnet. Gemäss der Experteninterviews sind die Aufgaben von IT-GRC am ehesten in der Service-Strategy-Phase und in der Service-Design-Phase anzutreffen.

Die Service-Strategy-Phase definiert die Strategie von IT-Services und legt nach Schlarman (2009, S. 15) basierend auf den Risiken und Vorgaben der Organisation die Ziele der IT-Services fest. Beispielsweise können Verantwortlichkeiten über RACI Matrizen dokumentiert werden. Da gemäss Kapitel 2.3.2.1 die Aufgaben vom Risk Management und Compliance Management im Interesse von Governance Bodies ausgeführt werden, können nach Schlarman (2009, S. 15) während der Service-Strategy-Phase die Governance Bodies gebildet und besetzt werden. Knoll und Strahringer (2017, S. 15) nennen exemplarisch ein IT-Risk Acceptance Board als Governance Body und erachten die Bildung eines Compliance Gremiums als notwendig, um die Einhaltung von internen und externen Vorgaben sicherzustellen. Gemäss der Experteninterviews stehen das Service Portfolio Management und Demand Management besonders im Fokus der IT-GRC Aufgaben. Die Service-Design-Phase plant die Erbringung von IT-Services. Gemäss der Experteninterviews betreffen die IT-GRC Aufgaben bei der Planung von IT-Services besonders das Service Continuity Management und Availability Management. In beiden Prozessen kommt der Berücksichtigung von Risiken und Vorgaben eine wichtige Rolle zu. Die Service-Transition-Phase überführt IT-Services in neuer oder in geänderter Form in produktive Systeme. Das Ziel der Service-Transition-Phase ist eine möglichst reibungslose Implementierung und eine möglichst vollständige Dokumentation der IT-Services. Es stellen sich hierbei die Fragen, wie Changes implementiert und damit IT-GRC Anforderungen adressiert werden (Schlarman, 2009, S. 15). Gemäss der Experteninterviews müssen im Change Management möglichst alle Changes auch auf Basis von Risiken und internen sowie externen Vorgaben geprüft und genehmigt werden. Die Service-Operation-Phase stellt den Betrieb von IT-Services sicher. Nach Schlarman (2009, S. 16) betreffen im Tagesbetrieb die IT-GRC Aufgaben das Event Management, Incident Management, Service Fulfillment, Problem Management und Access Management. Beispielsweise ist das Access Management an der Regelung der Verantwortlichkeiten beziehungsweise einer Segregation of Duties interessiert, damit die Vergabe von

Berechtigungen keine Risiken birgt oder nicht gegen Vorgaben verstösst (Schweizer, 2017). Auf Deutsch ist mit Segregation of Duties die Trennung von Verantwortlichkeiten gemeint (Schweizer, 2017). Die Service-Improvement-Phase sichert und überwacht fortlaufend die Qualität von IT-Services, um Verbesserungspotenziale zu erkennen. In dieser Phase werden die Kennzahlen der IT-Services gemessen, um deren Qualität im Auge zu behalten und das Management über den Erfolg oder über Abweichungen der IT-Services in Kenntnis zu setzen (Schlarman, 2009, S. 17). Als Hilfsmittel bietet sich beispielsweise die Verwendung einer Balanced Scorecard an, um die Wertschöpfung und die Leistungsergebnisse der IT zu messen (Schlarman, 2009, S. 17). Weiter werden beim Identifizieren der Optimierungsmöglichkeiten auch Rückmeldung einbezogen (Schlarman, 2009, S. 17). Dazu dient beispielsweise ein monatliches oder vierteljährliches Reporting als Stütze für die Adressierung von Verbesserungen (Schlarman, 2009, S. 17).

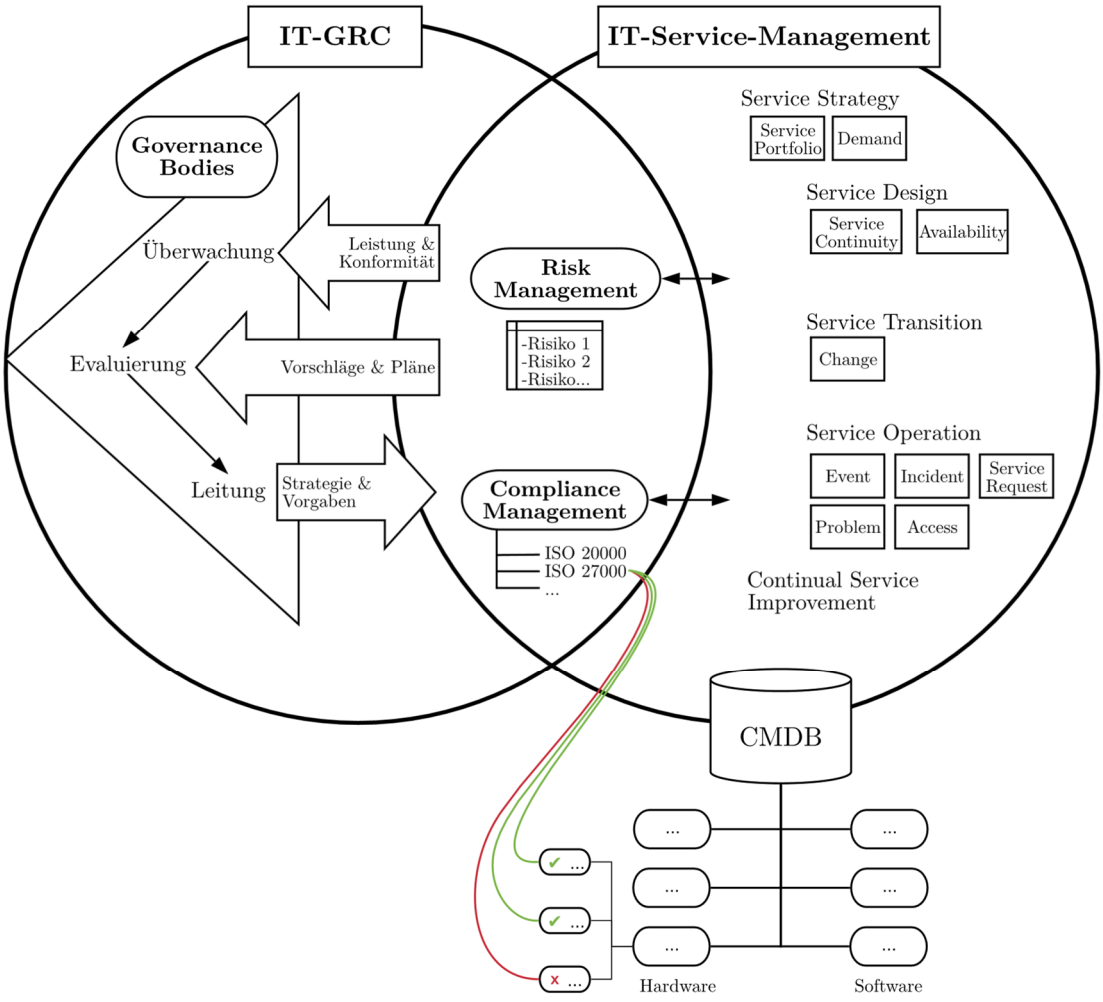


Abbildung 11: ITSM als Werkzeug für IT-GRC

3 Marktanalyse der ITSM Lösungsanbieter

Damit IT-Organisationen ITIL-basiertes ITSM ausüben beziehungsweise deren Effizienz steigern können, werden für IT-Organisationen ITSM Lösungen in unterschiedlicher Form und mit verschiedenen Funktionalitäten angeboten. ITSM Lösungen erleichtern die Aktivitäten und Prozesse im Zusammenhang mit der Definition, Planung, Implementierung, Ausführung und Optimierung von IT-Services (Gonzalez, Doheny, & Matchett, 2018, S. 1). Gonzalez, Doheny, & Matchett (2018, S. 1) halten fest, dass ITSM Lösungen überlebenswichtig für die Erbringung von IT-Services sind. Einige ITSM Lösungen ermöglichen die Nutzung von Funktionen, mit denen das Anwendungsgebiet von IT-GRC unterstützt werden kann. Um die Möglichkeiten und Grenzen von IT-GRC Funktionen in drei führenden ITSM Lösungen zu evaluieren, bedarf es einer Marktanalyse von ITSM Lösungen. Mit der Marktanalyse wird die zweite Teilfrage der Bachelorarbeit "*Welche führenden ITSM Lösungen werden am Markt angeboten?*" bearbeitet. In einem ersten Unterkapitel werden anhand von aktuellen Referenzen die derzeit führenden ITSM Lösungen erörtert und in einem zweiten Unterkapitel drei führende ITSM Lösungen für die Evaluierung ausgewählt und deren Anbieter vorgestellt.

3.1 Erhebung führender ITSM Lösungen

Pröhl & Zarnekow (2019) beschreiben den Markt von ITSM Lösungen als vielfältig und voluminös. Die ITSM Lösungsanbieter unterscheiden sich gemäss der Experteninterviews voneinander, indem einzelne, kleinere ITSM Lösungsanbieter sich auf einzelne Themen spezialisieren und Marktnischen für sich beanspruchen, wobei führende ITSM Lösungsanbieter wiederum möglichst das ganze Spektrum der IT-Organisation abdecken. Bisher vertrieben und realisierten Anbieter ITSM Lösungen On-Premises (Pröhl & Zarnekow, 2019). Aktuell stehen aufgrund der fortschreitenden Cloudtechnologien immer mehr ITSM Lösungen als Software as a Service (SaaS) zur Verfügung (Pröhl & Zarnekow, 2019). Neben der Verbreitung von SaaS vermarkten ITSM Lösungsanbieter nicht nur für IT-Organisationen Lösungen, sondern in Form von Enterprise Service Management (ESM) auch für ganze Unternehmen (Pröhl & Zarnekow, 2019). Zusätzlich zu den IT-Services von ITSM beinhaltet ESM unternehmensübergreifende Services, welche sich beispielsweise bei der Finanzbuchhaltung oder bei der Personalabteilung ansiedeln und Geschäftsprozesse durch die Unterstützung der IT automatisiert werden können.

Gonzalez et al. (2018) vom IT-Beratungsunternehmen Gartner haben für das Jahr 2018 ein Marktforschungsbericht über ITSM Lösungen in ihrem sogenannten Magic Quadrant erstellt. Pröhl & Zarnekow (2019) halten fest, dass mit dem Magic Quadrant von Gonzalez et al. (2018) die Unklarheiten zu den Marktführern von ITSM Lösungen behandelt werden. Vom Stand des 1. März 2018 wurden führende ITSM Lösungen unter Einhaltung von fünf Kriterien ausgewählt und anschliessend bewertet (Gonzalez et al., 2018). Das erste Auswahlkriterium erwartet von den ITSM Lösungen, dass Funktionen zum IT-Incident Management, Problem Management, Change Management, Configuration Management, Release Governance, IT-User Self-Service, IT-Knowledge Management, IT-Service Support Analytics & Reporting und SLA Management angeboten sowie ein grafischer Prozess-Designer unterstützt werden (Gonzalez et al., 2018). Das zweite Kriterium fordert, dass mindestens 35% der Kunden eine Version der ITSM Lösung nutzen, die nach dem 1. September 2016 publiziert wurde (Gonzalez et al., 2018). Das dritte Kriterium definiert einen jährlichen Mindestumsatz von 23 Millionen US-Dollar auf Basis der ITSM Lösung. Das vierte Kriterium umfasst die Lizenzvergabe der ITSM Lösung an mindestens 20 neuen Kunden im Jahr 2017, welche aufgrund eines einmaligen Kaufs einen Vertragswert von mindestens 300'000 US-Dollar oder aufgrund eines Abonnements einen jährlich Vertragswert von mindestens 150'000 US-Dollar aufweisen (Gonzalez et al., 2018). Das fünfte Kriterium stellt die letzte Anforderung, dass ein Vertriebsnetz inklusive zweier Niederlassungen in mindestens drei der folgenden Regionen besteht: Nordamerika, Lateinamerika, Afrika einschliesslich Naher Osten, Europa und Asien-Pazifik (Gonzalez et al., 2018).

Alle fünf Kriterien erfüllen die folgenden neun ITSM Lösungen: Axios Systems, BMC Software, CA Technologies, Cherwell Software, EasyVista, IBM, Ivanti, Micro Focus und ServiceNow. Gemäss der Abbildung 12 vergleichen Gonzalez et al. (2018) die neun führenden ITSM Lösungen anhand der Umsetzungsfähigkeit und der Vollständigkeit der Vision. Anhand des Vergleichs klassifizieren Gonzalez et al. (2018) die ITSM Lösungen in Leaders, Challengers, Niche Players und Visionaires. Auf der einen Seite fliessen in die Umsetzungsfähigkeit die Services der ITSM Lösung, die allgemeine wirtschaftliche Tragfähigkeit des ITSM Lösungsanbieters, die Preisgestaltung, die Reaktionsfähigkeit auf dem Markt, die Marketing-Umsetzung und die Kundenerfahrung ein (Gonzalez et al., 2018). Die Services der ITSM Lösung und die Preisgestaltung werden hoch gewichtet, wobei die restlichen Faktoren eine mittlere Gewichtung erhalten (Gonzalez et al., 2018). Auf der anderen Seite setzt sich die Vollständigkeit der Vision aus dem Marktverständnis,

der Marketingstrategie, der Verkaufsstrategie, der Produktstrategie, dem Geschäftsmodell, der Innovation und der Marktpräsenzstrategie zusammen (Gonzalez et al., 2018). Ausser der Verkaufsstrategie und dem Geschäftsmodell, die eine mittlere Gewichtung erhalten, werden alle restlichen Faktoren hoch gewichtet (Gonzalez et al., 2018). BMC Software und ServiceNow weisen als Marktführer eine hohe Umsetzungsfähigkeit und Vollständigkeit der Vision auf und werden als Leader spezifiziert (vgl. Abbildung 12). Anlässlich der hohen Umsetzungsfähigkeit und der mittleren Vollständigkeit der Vision werden Cherwell Software und Ivanti als Challenger eingestuft, die an der Grenze zur Kategorie Leader stehen (vgl. Abbildung 12). Gonzalez et al. (2018) ordnen die restlichen fünf ITSM Lösungen als Niche Player ein.

Abbildung 12: Magic Quadrant für ITSM Lösungen (Gonzalez et al., 2018)

Neben Gonzalez et al. (2018) haben im Jahr 2018 Betz et al. (2018) vom Unternehmen Forrester Research, welches Marktforschungen und Analysen in Bezug zur IT durchführt, ebenfalls den Markt um ITSM Lösungen analysiert. Konkret wurden im "*The Forrester Wave*"-Bericht von Betz et al. (2018) die ITSM Lösungen von Atlassian, Axios, BMC Software, CA Technologies, Cherwell Software, EasyVista, IBM, Ivanti, Micro Focus, ServiceNow, SunView und TOPdesk gemäss der Abbildung 13 geprüft. In der Prüfung von Betz et al. (2018) wurden auf der einen Seite die Stärke der Strategie und auf der anderen Seite die Stärke des Angebots beurteilt. Die Auswertung der Beurteilung ordnet die ITSM Lösungen gemäss der Abbildung 13 einer der vier Kategorien Leaders, Strong Performers, Contender und Challenger zu. Die Prüfung hat ergeben, dass ServiceNow sowie Cherwell Software als Leader und BMC Software sowie Ivanti als Strong Performer zu klassifizieren sind (vgl. Abbildung 13).

Abbildung 13: The Forrester Wave für ITSM Lösungen (Betz et al., 2018)

3.2 Selektion drei führender ITSM Lösungen

Das Ziel dieser Bachelorarbeit ist die Evaluierung der Mächtigkeit und der Limitation von führenden ITSM Lösungen hinsichtlich der IT-GRC Funktionen. Im Rahmen dieser Bachelorarbeit beläuft sich die Zahl der Evaluierung auf drei ITSM Lösungen, um ein möglichst repräsentatives Ergebnis zu ermitteln und einen Vergleich zwischen den einzelnen ITSM Lösungen ziehen zu können.

In einem ersten Schritt werden für ein möglichst repräsentatives Ergebnis von führenden ITSM Lösungen drei der neun führenden ITSM Lösungen ausgewählt, welche die von Gonzalez et al. (2018) vom IT-Beratungsunternehmen Gartner definierten fünf Kriterien aus dem Kapitel 3.1 erfüllen und kumuliert die höchsten Werte in der Umsetzungsfähigkeit und der Vollständigkeit gemäss der Abbildung 12 erzielen. In einem zweiten Schritt fliessen in der Kumulation zur Abbildung 9 die Stärke der Strategie und die Stärke des Angebots der Abbildung 13, welche von Betz et al. (2018) vom Unternehmen Forrester Research ermittelt wurden. BMC Software, Cherwell Software, Ivanti und ServiceNow werden als führende ITSM Lösungen favorisiert.

In erster Linie kommen jedoch nur jene führenden ITSM Lösungen in die engere Auswahl, von denen die Anbieter Hands-On-Demos und Testzugänge für die Evaluierung von IT-GRC Funktionen im zeitlichen Rahmen der Bachelorarbeit bereitstellen und ihre IT-GRC Funktionen präsentieren. Durch Hands-On-Demos und Testzugänge sowie der Präsentationen der ITSM Lösungsanbieter wird eine umfassendere Evaluierung der IT-GRC Funktionen ermöglicht, als dass die IT-GRC Funktionen nur mit Produktdokumentationen geprüft werden.

Nach Abklärungen mit den favorisierten ITSM Lösungsanbietern zur Bereitstellung von Hands-On-Demos, Testzugängen und Präsentationen verbleiben die ITSM Lösungen von Cherwell Software, Ivanti und ServiceNow, für die eine Evaluierung der IT-GRC Funktionen erfolgen kann. BMC Software konnte die Anforderungen im zeitlichen Rahmen der Bachelorarbeit nicht erfüllen.

4 Ausarbeitung des Bewertungskatalogs

Für die Bewertung von IT-GRC Funktionen der einzelnen ITSM Lösungen wird die Methodik der Nutzwertanalyse eingesetzt. Um eine Nutzwertanalyse durchzuführen, besteht der Bedarf nach einem Katalog, wo die Bewertungskriterien ausgelegt werden. Die Bewertungskriterien, mit denen der Einsatz von IT-GRC Funktionen in den drei ausgewählten ITSM Lösungen evaluiert und gemessen werden, sind im Voraus auszuarbeiten und zu definieren. Dieses Kapitel beschäftigt sich mit der Erhebung der Bewertungskriterien, um damit die erhobenen Bewertungskriterien auszulegen und den Rahmen für die Evaluierung zu bilden. In der Ausarbeitung des Bewertungskatalogs fliessen neben wissenschaftlichen Quellen auch Experteninterviews ein. Die Zielsetzung für den Einbezug von Experteninterviews liegt darin, mit den Erfahrungswerten der Experten die Bewertungskriterien von IT-GRC Funktionen zu definieren. Aus diesem Kapitel resultiert schlussendlich ein Bewertungskatalog für die Evaluierung der IT-GRC Funktionen von führenden ITSM Lösungen.

Nach Online-Recherchen finden sich verschiedene wissenschaftliche Artikel, die Kriterien für die Bewertung unterschiedlicher Lösungen definieren. Hingegen lässt sich keine Literatur ausfindig machen, welche sich spezifisch auf die Bewertungskriterien von IT-GRC Funktionen in ITSM Lösungen fokussiert. In einem wissenschaftlichen Artikel haben Rouhani und Ravasan (2014, S. 7 ff.) 46 Kriterien zusammengetragen und in Kategorien gruppiert, mit denen sich ITSM Lösungen prüfen und bewerten lassen. Von allen definierten 46 Kriterien spezifizieren Rouhani und Ravasan (2014, S. 7 ff.) 25 in funktionale und 21 in nicht-funktionale Kriterien. Funktionale Kriterien bewerten die Unterstützung der Funktionen für das Aufgabengebiet, für welches es konzipiert wurde. Nichtfunktionalen Kriterien beziehen sich auf die Qualitätsmerkmale der angebotenen Funktionen (Rouhani & Ravasan, 2014, S. 7 ff.). Die von Rouhani und Ravasan (2014, S. 7 ff.) gelisteten 25 funktionalen Kriterien werden nicht weiter berücksichtigt, da sich deren Funktionalitäten auf das Aufgabengebiet von ITSM Lösungen konzentrieren und zum spezifischen Themengebiet von IT-GRC Funktionen abweichen. Anhand dieser Ausgangslage werden Experten konsultiert und weitere wissenschaftliche Artikel beigezogen, wo sich die Kriterien für die Bewertung von IT-GRC Funktionen in ITSM Lösungen gemäss der Tabelle 1 ableiten lassen. Die Tabelle 1 wird in funktionale und nicht-funktionale Kriterien aufgeteilt und in den entsprechenden Unterkapiteln konkretisiert.

		Kriterien	
Funktionale Kriterien	Risk Management	Definition des Risikoappetits	R1
		Verwaltung von Risikopraktiken	R2
		Bewertung von Risiken	R3
		Monitoring der Risiken	R4
		Auditabdeckung	R5
	Compliance Management	Verwaltung von Vorgaben	C1
		Regelung der Verantwortlichkeiten	C2
		Überprüfung der Vorgabenverwaltung	C3
		Monitoring der Compliance	C4
		Ausnahmeregelung	C5
Nicht-funktionale Kriterien		Effizienz	N1
		Usability	N2
		Zuverlässigkeit	N3
		ITSM Lösungsanbieter	N4
		Lizenzierungsmodell	N5

Tabelle 1: Bewertungskriterien für IT-GRC Funktionen in ITSM Lösungen

4.1 Erhebung funktionaler Kriterien

Die ISO/IEC 25010 definiert die Anforderungen an die Funktionalität, dass die Vollständigkeit, Korrektheit und Angemessenheit für das betroffene Aufgabengebiet gegeben sein müssen. Gemäss der Experteninterviews bilden das Risk Management und Compliance Management das Aufgabengebiet, welches in ITSM Lösungen automatisiert werden kann. Entsprechend beziehen sich die funktionalen Kriterien auf Funktionen von ITSM Lösungen, welche die Erledigung der Aufgaben eines Risk Managements und eines Compliance Managements durch ITSM Lösungen bewerten. Die Aufgaben des Risk Managements und Compliance Managements, welche in Kapitel 2.3.2 erörtert wurden, dienen somit als Kriterien. Die Bewertung dieser Kriterien wird im nächsten Schritt erläutert.

Gemäss der Tabelle 1 werden ITSM Lösungen im Bereich vom Risk Management unter anderem daran gemessen, wie die Definition des Risikoappetits des Unternehmens funktional abgedeckt wird. Für die Definition des Risikoappetits wird in den ITSM Lösungen eine Möglichkeit zur Dokumentation erwartet. Die Definition des Risikoappetits legt den Grundstein für die Identifizierung von Risiken. Damit überhaupt Risiken in der ITSM Lösung erfasst werden können, müssen Funktionen zur Identifizierung und Bewertung von Risiken vorhanden sein. Bei der Erfassung der Risiken spielt vor allem die Bewertung eine zentrale Rolle. Zum Beispiel soll die Risikobewertung die Eintrittswahrscheinlichkeit und das Schadensausmass berechnen können, um damit die Priorität festzulegen. Weiter wird in den ITSM Lösungen erwartet, dass Risiken mithilfe von Dashboards verfolgt werden und entsprechende Visualisierungswerkzeuge wie Risk Matrizen oder Heat Maps zur Verfügung stehen. Da die Auditabdeckung auch eine Relevanz für IT-GRC Funktionen aufweist und gemäss Kapitel 2.3.2 im Risk Management untergebracht wird, werden die Möglichkeiten zur Erfassung und Verwaltung von Audits analysiert. Die Anforderungen an die funktionalen Kriterien vom Risk Management werden in der Tabelle 2 als Bewertungskatalog ausgelegt. In der Punktevergabe wird 5 als höchste Anforderung und 1 als niedrigste Anforderung eines Kriteriums definiert.

Punkte	Anforderungen für Kriterium R1: **Definition des Risikoappetits**
1	Der Risikoappetit kann nicht definiert werden.
2	Der Risikoappetit kann manuell definiert werden.
3	Der Risikoappetit kann über IT-GRC Funktionen definiert werden.
4	Der Risikoappetit kann über IT-GRC Funktionen definiert und später mit Risiken verknüpft werden.
5	Der Risikoappetit lässt sich über IT-GRC Funktionen definieren, später mit Risiken verknüpfen und überprüfen.
Punkte	Anforderungen für Kriterium R2: **Verwaltung von Risikopraktiken**
1	Risikopraktiken können nicht definiert werden.
2	Risikopraktiken können definiert werden.
3	Risikopraktiken können definiert und einem Risiko hinterlegt werden.
4	Risikopraktiken können sowohl definiert und einem Risiko hinterlegt werden als auch einem Genehmigungsprozess unterstehen.
5	Risikopraktiken können sowohl definiert und einem Risiko hinterlegt werden als auch einem Genehmigungsprozess unterstehen und an Risikoverantwortliche zugewiesen werden.
Punkte	Anforderungen für Kriterium R3: **Bewertung von Risiken**
1	Risiken können nicht definiert werden.

2	Risiken können definiert werden, wobei eine Risikobewertung nicht ermöglicht wird.
3	Risiken können definiert und bewertet beziehungsweise eingestuft werden.
4	Risiken können definiert und anhand eines Fragekatalogs bewertet beziehungsweise eingestuft werden.
5	Risiken können definiert und anhand eines Fragekatalogs bewertet werden. Eine Einstufung des Risikos findet über eine Berechnung der Eintrittswahrscheinlichkeit und des Schadensausmasses statt.
Punkte	Anforderungen für Kriterium R4: **Monitoring der Risiken**
1	Es existieren keine Dashboards oder exportierbare Berichte zu Risiken.
2	Es existieren entweder Dashboards oder exportierbare Berichte zu Risiken.
3	Es existieren sowohl Dashboards als auch exportierbare Berichte zu Risiken.
4	Es existieren sowohl Dashboards als auch exportierbare Berichte zu Risiken, wobei entweder Dashboards oder exportierbare Berichte personalisierbar sind.
5	Es existieren sowohl Dashboards als auch exportierbare Berichte zu Risiken, die personalisierbar sind.
Punkte	Anforderungen für Kriterium R5: **Auditabdeckung**
1	Die funktionale Erfassung von Audits wird nicht ermöglicht.
2	Die funktionale Erfassung von Audits wird ermöglicht.
3	Die funktionale Erfassung von Audits und die Zuordnung von Verantwortlichen wird ermöglicht.
4	Die funktionale Erfassung von Audits, die Zuordnung von Verantwortlichen und die Hinterlegung von Steuerelementen werden ermöglicht.
5	Die funktionale Erfassung von Audits, die Zuordnung von Verantwortlichen und die Hinterlegung von Steuerelementen werden ermöglicht. Eine automatisierte Überwachung der Audits ist funktional abgedeckt.

Tabelle 2: Bewertungskatalog für funktionale Kriterien zum Risk Management

Im Bereich des Compliance Managements wird zum einen jene Funktionen bewertet, welche zur Erfassung sowie zur Durchsetzung von internen und externen Vorgaben beitragen. In den Experteninterviews wird die Anforderung genannt, beispielsweise die ISO 20000, ISO 27000 oder weitere Regelwerke in der ITSM Lösung aus zentraler Quelle als Auswahl zur Verfügung gestellt zu bekommen. Aufgrund der Auswahl soll der Kunde die passenden Bestandteile als Set zusammenstellen können, um Vorgaben abzuleiten. Weiter sollen Verantwortlichkeiten dokumentiert werden können, um und beispielsweise RACI-Matrizen abzubilden. Sowohl Abnehmer als auch die Besetzung von Governance Bodies sollen bei der Regelung der Verantwortlichkeiten berücksichtigt werden. Im

Compliance Managements sollen temporär Ausnahmen definiert, attestiert und dokumentiert werden können. Weiter soll eine IT-GRC Funktion bestehen, welche die Genehmigung temporärer Ausnahmeregelungen dokumentiert. Dashboards und exportierbare Berichte werden als wichtige Bestandteile der Überwachung genannt. Beispielsweise sollen einmal jährlich oder monatlich Stichproben aus der Datenbank entnommen werden können, um Autorisierungen zu überprüfen. Die Anforderungen an die funktionalen Kriterien vom Compliance Management sind in der Tabelle 3 als Bewertungskatalog definiert.

Punkte	Anforderungen für Kriterium C1: **Verwaltung von Vorgaben**
1	Vorgaben können nicht definiert werden.
2	Vorgaben können manuell erfasst werden.
3	Vorgaben können manuell erfasst und Verantwortlichen zugeordnet werden.
4	Vorgaben können manuell erfasst sowie Steuerelementen und Verantwortlichen zugeordnet werden.
5	Vorgaben lassen sich aus Regelwerken, die vom ITSM Lösungsanbieter zentral gepflegt und zur Verfügung gestellt werden, ableiten und können sowohl Steuerelementen als auch Verantwortlichen zugeordnet werden.
Punkte	Anforderungen für Kriterium C2: **Regelung der Verantwortlichkeiten**
1	Verantwortlichkeiten können nicht definiert werden.
2	Verantwortlichkeiten können manuell definiert werden.
3	Verantwortlichkeiten können definiert und entweder Vorgaben oder Risiken hinterlegt werden.
4	Verantwortlichkeiten können definiert und Vorgaben sowie Risiken zugeordnet werden.
5	Verantwortlichkeiten können definiert, verfolgt, dokumentiert und Vorgaben sowie Risiken zugeordnet werden. Die Segregation of Duties wird funktional unterstützt.
Punkte	Anforderungen für Kriterium C3: **Überprüfung der Vorgabenverwaltung**
1	Es besteht keine Vorgabenverwaltung.
2	Es besteht eine Vorgabenverwaltung, deren Überprüfung jedoch funktional nicht unterstützt wird.
3	Es besteht eine Vorgabenverwaltung, deren Überprüfung funktional unterstützt wird, jedoch manuell durchgeführt werden muss.
4	Es besteht eine Vorgabenverwaltung und eine funktionale Überprüfung, da die Vorgaben automatisiert gemessen werden.
5	Es besteht eine Vorgabenverwaltung und eine funktionale Überprüfung mit vorgefertigten Vorlagen, da die Vorgaben automatisiert gemessen werden.
Punkte	Anforderungen für Kriterium C4: **Monitoring der Compliance**
1	Es existieren keine Dashboards oder exportierbare Berichte zur Compliance.

2	Es existieren entweder Dashboards oder exportierbare Berichte zur Compliance.
3	Es existieren sowohl Dashboards als auch exportierbare Berichte zur Compliance.
4	Es existieren sowohl Dashboards als auch exportierbare Berichte zur Compliance, wobei entweder Dashboards oder exportierbare Berichte personalisierbar sind.
5	Es existieren sowohl Dashboards als auch exportierbare Berichte zur Compliance, die personalisierbar sind.
Punkte	Anforderungen für Kriterium C5: **Ausnahmeregelung**
1	Ausnahmeregelungen können nicht definiert werden.
2	Ausnahmeregelungen können definiert werden.
3	Ausnahmeregelungen können mit Fristen definiert werden.
4	Ausnahmeregelungen können mit Fristen definiert werden und unterstehen einem Genehmigungsprozess.
5	Ausnahmeregelungen können mit Fristen definiert werden, unterstehen einem Genehmigungsprozess und können Vorgaben zugeordnet werden.

Tabelle 3: Bewertungskatalog für funktionale Kriterien zum Compliance Management

4.2 Erhebung nicht-funktionaler Kriterien

Rouhani und Ravasan (2014, S. 7 ff.) unterteilen die 21 nicht-funktionalen Kriterien in Qualität, Technik, ITSM Lösungsanbieter und Implementierung. Auf Basis der ISO/IEC 9126 fassen Rouhani und Ravasan (2014, S. 7 ff.) die Zuverlässigkeit, die Usability, die Wartbarkeit, die Leistungsfähigkeit, die Personalisierbarkeit und die Portabilität als qualitative Kriterien zusammen, wobei das Kommunikationsprotokoll, die Plattformen, das Datenbankmanagementsystem, die Programmiersprache, die Dokumentation, die Standardkonfigurationen und die Sicherheit die technischen Kriterien bilden. Da die ISO/IEC 9126 durch die ISO/IEC 25010 ersetzt wurde, werden die qualitativen und technischen von Rouhani und Ravasan (2014, S. 7 ff.) durch die ISO/IEC 25010 adaptiert. Zusätzlich zur ISO/IEC 9126 wurden von Rouhani und Ravasan (2014, S. 7 ff.) die Kriterien des ITSM Lösungsanbieters einbezogen, die sich aus der Reputation, der Schulung sowie dem Support, der Erfahrung und dem Beratungsdienst des ITSM Lösungsanbieters zusammensetzt. Weiter nehmen Rouhani und Ravasan (2014, S. 7 ff.) abweichend von der ISO/IEC 9126 Rücksicht auf die Kosten der ITSM Lösungen. Auch in den Experteninterviews wird die Wirtschaftlichkeit zu den relevanten Kriterien gezählt. Da der Fokus der Bachelorarbeit auf die Evaluierung von IT-GRC Funktionen anhand von funktionalen Kriterien liegt, werden nicht-funktionale Kriterien gebündelt. Der Bewertungskatalog definiert aus diesem Grund die Effizienz, die Usability, die Zuverlässigkeit der ITSM

Lösungsanbieter und das Lizenzierungsmodell als nicht-funktionale Kriterien gemäss der Tabelle 1. Die Effizienz prüft die Wirksamkeit beziehungsweise die Leistung der IT-GRC Funktionen. Die Effizienz wird am Zeitverhalten der Hands-On-Demos und Testzugänge gemessen. Die Usability befasst sich mit der Ergonomie der IT-GRC Funktionen, welcher die Erkennbarkeit, Lernfähigkeit, Bedienbarkeit, Schutz vor Benutzerfehlbedienung, Ästhetik der Benutzeroberfläche und Zugänglichkeit zugeordnet sind. Die Zuverlässigkeit umfasst die Reife, die Fehlertoleranz und die Wiederherstellbarkeit der IT-GRC Funktionen. Auch in der Bewertung der Zuverlässigkeit dienen die Hands-On-Demos und Testzugänge als Grundlage. Die Messung erfolgt durch das händische Durchführen von Anwendungsfällen aller IT-GRC Funktionen. Die ITSM Lösungsanbieter werden anhand der Marktposition und Produktdokumentation bewertet. Die Anforderungen an die nichtfunktionalen Kriterien werden in der Tabelle 4 als Bewertungskatalog ausgelegt.

Punkte	Anforderungen für Kriterium N1: **Effizienz**
1	Die Effizienz der ITSM Lösung und der IT-GRC Funktionen lässt keine akzeptable Bedienung zu.
2	Die Effizienz der ITSM Lösung lässt eine akzeptable Bedienung zu, wobei die Effizienz der IT-GRC Funktionen keine akzeptable Bedienung zulässt.
3	Die Effizienz der ITSM Lösung und der IT-GRC Funktionen lässt eine akzeptable Bedienung zu.
4	Die Effizienz der ITSM Lösung lässt eine dynamische und die Effizienz der IT-GRC Funktionen lässt eine akzeptable Bedienung zu.
5	Die Effizienz der ITSM Lösung und der IT-GRC Funktionen lassen eine dynamische Bedienung zu.
Punkte	Anforderungen für Kriterium N2: **Usability**
1	Die Erkennbarkeit, Lernfähigkeit, Bedienbarkeit, Schutz vor Benutzerfehlbedienung, Ästhetik der Benutzeroberfläche und Zugänglichkeit der ITSM Lösung sind ungenügend zu werten.
2	Die Erkennbarkeit, Lernfähigkeit, Bedienbarkeit, Schutz vor Benutzerfehlbedienung, Ästhetik der Benutzeroberfläche und Zugänglichkeit der ITSM Lösung genügen den Minimalansprüchen, wobei jene der IT-GRC Funktionen ungenügend sind.
3	Die Erkennbarkeit, Lernfähigkeit, Bedienbarkeit, Schutz vor Benutzerfehlbedienung, Ästhetik der Benutzeroberfläche und Zugänglichkeit der ITSM Lösung sowie der IT-GRC Funktionen genügen den Minimalansprüchen.
4	Die Erkennbarkeit, Lernfähigkeit, Bedienbarkeit, Schutz vor Benutzerfehlbedienung, Ästhetik der Benutzeroberfläche und Zugänglichkeit der ITSM Lösung sowie der IT-GRC Funktionen genügen den Minimalansprüchen und ermöglichen unter anderem eine einfache Personalisierung.
5	Die Erkennbarkeit, Lernfähigkeit, Bedienbarkeit, Schutz vor Benutzerfehlbedienung, Ästhetik der Benutzeroberfläche und Zugänglichkeit der ITSM Lösung sowie

	der IT-GRC Funktionen genügen den Minimalansprüchen und ermöglichen unter anderem eine umfassende Personalisierung.
Punkte	Anforderungen für Kriterium N3: **Zuverlässigkeit**
1	Die ITSM Lösung sowie der IT-GRC Funktionen weisen eine ungenügend Reife auf, weshalb keine zuverlässige Bedienung möglich ist.
2	Die Reife der ITSM Lösung ist genügend, wobei die IT-GRC Funktionen ungenügende Reife aufweisen und keine zuverlässige Bedienung zulassen.
3	Die Reife der ITSM Lösung sowie der IT-GRC Funktionen ist genügend zu werten.
4	Die ITSM Lösung weist eine fortgeschrittene Reife auf, wobei die Reife der IT-GRC Funktionen genügend zu werten ist.
5	Die ITSM Lösung sowie die IT-GRC Funktionen weisen eine fortgeschrittene Reife auf.
Punkte	Anforderungen für Kriterium N4: **ITSM Lösungsanbieter**
1	Der ITSM Lösungsanbieter stellt keine Produktdokumentation zu IT-GRC Funktionen zur Verfügung und gilt im Markt für ITSM Lösungen als Niche Player.
2	Der ITSM Lösungsanbieter stellt eine einfache Produktdokumentation zu IT-GRC Funktionen zur Verfügung und gilt im Markt für ITSM Lösungen als Niche Player.
3	Der ITSM Lösungsanbieter stellt eine einfache Produktdokumentation zu IT-GRC Funktionen zur Verfügung und gilt im Markt für ITSM Lösungen als Challenger.
4	Der ITSM Lösungsanbieter stellt eine umfassende Produktdokumentation zu IT-GRC Funktionen zur Verfügung und gilt im Markt für ITSM Lösungen als Challenger.
5	Der ITSM Lösungsanbieter stellt eine umfassende Produktdokumentation zu IT-GRC Funktionen zur Verfügung und gilt im Markt für ITSM Lösungen als Leader.
Punkte	Anforderungen für Kriterium N5: **Lizenzierungsmodell**
1	Das Lizenzierungsmodell ist nicht bekannt.
2	Das Lizenzierungsmodell basiert auf flexibel gestaltete Preise der ITSM Lösung und der IT-GRC Funktionen.
3	Das Lizenzierungsmodell der ITSM Lösung ist flexibel gestaltet, wobei die IT-GRC Funktionen keine zusätzlichen Lizenzkosten generieren.
4	Das Lizenzierungsmodell definiert sich anhand der Benutzeranzahl der ITSM Lösung und der IT-GRC Funktionen.
5	Das Lizenzierungsmodell für die ITSM Lösung definiert sich anhand der Benutzeranzahl. Die IT-GRC Funktionen verursachen keine zusätzlichen Lizenzkosten.

Tabelle 4: Bewertungskatalog für nicht-funktionale Kriterien

5 Evaluierung der ITSM Lösungen

Dieses Kapitel evaluiert die IT-GRC Funktionen der drei führenden ITSM Lösungen von Cherwell Software, Ivanti und ServiceNow. Auf der einen Seite bilden der Bewertungskatalog mit dessen Bewertungskriterien die Grundlage für die Evaluierung und auf der anderen Seite sind Produktdokumentationen, Hands-On-Demos sowie Testzugänge Gegenstand der Evaluierung, welche zusammen eine fundierte Einsicht auf die IT-GRC Funktionen der jeweiligen ITSM Lösungen gewähren. Jeder ITSM Lösungsanbieter führte zusätzlich eine Präsentation durch, um die Evaluierung zu festigen und damit über alle drei führenden ITSM Lösungsanbietern eine möglichst gleiche Informationsqualität besteht.

5.1 Evaluierung der IT-GRC Funktionen von Cherwell Software

Für die Evaluierung der IT-GRC Funktionen in führenden ITSM Lösungen wird Cherwell Software als erster ITSM Lösungsanbieter ausgewählt. Cherwell Software wurde im Jahr 2004 in den USA gegründet (Bloomberg, 2019a). Der Sitz von Cherwell Software befindet sich in Colorado Springs, Colorado (Bloomberg, 2019a). Cherwell Software bietet die ITSM Lösung mit der Bezeichnung Cherwell Service Management beziehungsweise CSM an, welche sowohl über SaaS als auch über On-Premises betrieben wird (Bloomberg, 2019a). CSM richtet sich an Unternehmen mit einem mittleren I/O-Reifegrad (Gonzalez et al., 2018). Gonzalez et al. (2018) heben bei CSM hervor, dass im Jahr 2018 ein hohes Kundenengagement und damit eine treue Anhängerschaft von zufriedenen Kunden erzielt wurde. Weiter nennen Gonzalez et al. (2018), dass Erweiterungen durch Drittanbieter oder der Community in CSM über die sogenannte *mergeable Application* (mApp)-Schnittstelle implementiert werden und die Anzahl dieser Implementationen stetig wächst. Gemäss Gonzalez et al. (2018) ermöglicht die mApp-Schnittstelle Cherwell Software, sich flexibler an die Bedürfnisse der Kunden zu richten. Cherwell Software (2019b) bietet in CSM das Modul Information Security Management System (ISMS) als mApp-Erweiterung an, welches sowohl IT-GRC Funktionen als auch IT-Security Funktionen enthält. Das Modul wird kostenlos heruntergeladen und out of the box in CSM eingesetzt. Online besteht zum Modul ISMS eine Produktdokumentation und ein einstündiger Videokurs. In der Produktdokumentation werden Anleitungen für die einzelnen Funktionen des Moduls bereitgestellt. Die Effizienz sowie Zuverlässigkeit von CSM ist auf Grundlage der Evaluierung sehr hoch zu werten, wobei die Usability mittelmässig zu werten ist. Die Funktionen von CSM, welche die Ausübung von IT-GRC unterstützen, bestehen aus

dem Erfassen von Steuerelementen, internen Vorgaben, Regelwerken, externen Vorgaben, Risikobewertungen und Ausnahmeregelungen. Weiter können Audits koordiniert sowie über ein Dashboard die Zustände vom Risk Management und Compliance Management überwacht werden. Steuerelemente beziehen sich auf die Verwaltung der Nutzung oder auf die Verwaltung des Verhaltens eines Geräts, Systems oder Service (Steinberg, 2011, S. 124). Gemäss Steinberg (2011, S. 124) darf die einfache Handhabung von Geräten, Systemen oder Services nicht mit Steuerelementen gleichgesetzt werden. Für die Nutzung von Steuerelementen muss gemäss Steinberg (2011, S. 124) sichergestellt werden, dass der Output den Vorgaben entspricht und dass die Aktivitäten sowie die Vorgaben zu den Aktivitäten definiert und genehmigt sind.

Als erste IT-GRC Funktion werden Steuerelemente in CSM entweder in der Tabelle aller Steuerelement-Datensätze mit einem neuen Eintrag erfasst oder bei grösserer Anzahl über eine Datei im Comma Separated Values (CSV) Format importiert. In CSM werden Steuerelemente mit Authority Documents, Citations oder Policies verknüpft. Die Begriffe Authority Document, Citation und Policy stehen in CSM für Regelwerke, externe Vorgaben und interne Vorgaben. Gemäss der Abbildung 14 sind Authority Documents die Regelwerke, aus denen externe Vorgaben extrahiert werden. Die externen Vorgaben werden in CSM als Citations erfasst. Die Policies bilden gemäss der Abbildung 14 die internen Vorgaben. Die Zuordnung zu Steuerelementen erfolgt, um die internen und externen Vorgaben der einzelnen Steuerelemente zu messen und um daraus die Compliance abzuleiten.

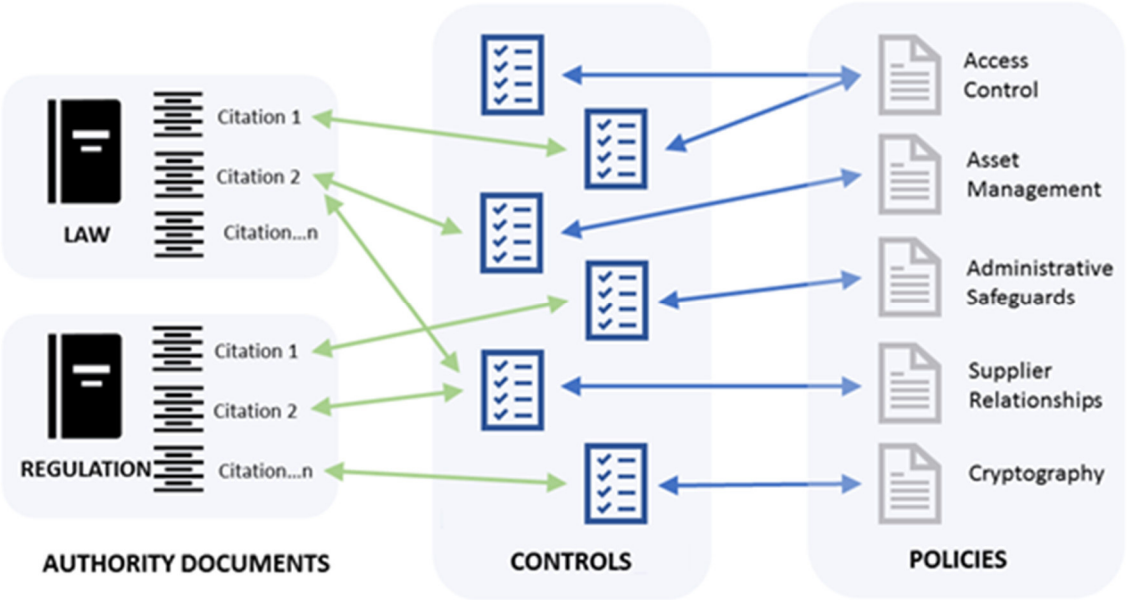


Abbildung 14: Abhängigkeit von Vorgaben (Cherwell Software, 2019b)

Bei der Erfassung von internen Vorgaben werden als zweite IT-GRC Funktion in CSM zuerst der Titel, die Beschreibung und die Verantwortlichkeiten gemäss der Abbildung 15 hinterlegt. Auch werden Businessverantwortliche den internen Vorgaben zugeordnet. Danach können der internen Vorgabe das entsprechende Asset, die Priorität, die Daten vom Projektstart und -ende, die Überprüfungsfrequenz sowie weitere Informationen zugeordnet werden. Die interne Vorgabe ist anschliessend aktiv, kann jedoch zu einem späteren Zeitpunkt wieder angepasst oder zurückgezogen werden.

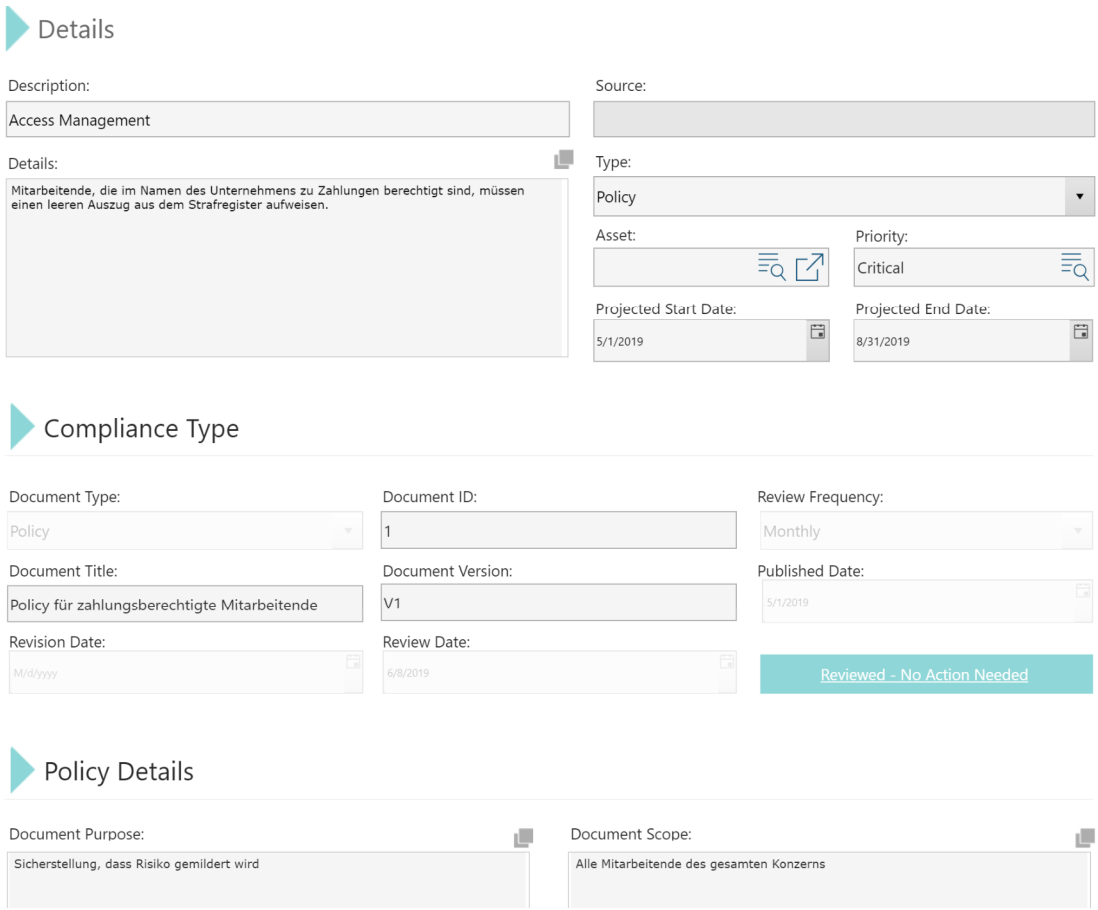


Abbildung 15: Erfassung von Vorgaben in CSM

Die dritte IT-GRC Funktion von CSM ist die Erfassung von Regelwerken. Analog zur Erfassung von internen Vorgaben werden bei Regelwerken der Titel, die Beschreibung und die Verantwortlichkeiten hinterlegt. Anstelle der Businessverantwortlichen werden die Prozessverantwortliche und die Urheber den Regelwerken zugeordnet. CSM bietet bei der Definition der Regelwerke die Optionen, den Typ der Regelwerke entweder als vertragliche Verpflichtung, als internationale oder nationale Norm, als Regulierung, als Regulierungsleitfaden oder als Statut zu klassifizieren. Die Erfassung von externen Vorgaben ist die vierte IT-GRC Funktion und erfolgt gleich wie bei Steuerelementen, indem

entweder in der Tabelle der externen Vorgaben ein neuer Eintrag erfasst oder mehrere Einträge via einer CSV-Datei importiert werden. Einer externen Vorgabe wird der Titel, die Beschreibung und die Zuordnung zu einem Regelwerk angegeben. Weiter besteht die Option, zwischen der Erforderlichkeit oder Nichterforderlichkeit eines Nachweises zu wählen, wobei bei beiden Optionen eine Rechtfertigung hinterlegt werden kann. Bei der Wahl der Erforderlichkeit eines Nachweises wird automatisiert geprüft, ob die externe Vorgabe mindestens mit einem Steuerelement und das Steuerelement mit mindestens einer internen Vorgabe verbunden ist.

Die Erfassung von Risikobewertungen hinterlegt als fünfte IT-GRC Funktion zuerst generelle Informationen zu einem Risiko und weist dem Risiko unter anderem das zu bewertende Asset, den Asset-Owner oder den Risk-Owner gemäss der Abbildung 16 zu. Nach den Zuweisungen wird die Datenklassifizierung angegeben, welche von öffentlich bis vertraulich reicht. Im nächsten Schritt sind Fragen zu den drei Themen der Datenklassifizierung, der Gefahrenanalyse und der Risikominderung zu beantworten. Mit der Beantwortung aller Fragen wird das Risiko berechnet. Es werden Massnahmen gemäss der Abbildung 17 entschieden, um das Risiko zu behandeln. Als Optionen stehen entweder das Akzeptieren, Vermeiden, Übertragen oder Verringern des Risikos zur Auswahl. Die Verringerung des Risikos kann durch Steuerelemente verwaltet werden. Nach dem Abschluss der Erfassung kann die Risikobewertung verfolgt werden, um beispielsweise nach der Umsetzung von Massnahmen die Risikobewertung zu aktualisieren oder gänzlich zurückzuziehen. CSM ermöglicht die Erfassung von Ausnahmeregelungen als sechste IT-GRC Funktion. Ausnahmeregelungen werden in CSM eingegeben, um die Nichteinhaltung eines Audits, Risikos oder einer internen Vorgabe zu dokumentieren und zu genehmigen. Entsprechend wird bei der Erfassung einer Ausnahmeregelung in einem ersten Schritt ausgewählt, ob es sich um ein Audit, Risiko oder eine interne Vorgabe handelt. Je nach Auswahl werden die Verantwortlichkeiten unterschiedlich zugewiesen und die Dauer der Ausnahmeregelung angegeben. Sobald in einem weiteren Schritt beschrieben wird, weshalb die Ausnahmeregelung in Kraft treten soll, ein Configuration Item ausgewählt wurde oder weitere Informationen hinterlegt sind, wird die Ausnahmeregelung gespeichert und die verantwortlichen Personen informiert. Die verantwortlichen Personen genehmigen die Ausnahmeregelung, verweigern diese oder enthalten sich. Nach der Genehmigung gilt die Ausnahmeregelung bis zur angegebenen Dauer oder bis die Ausnahmeregelung vorher zurückgezogen wird.

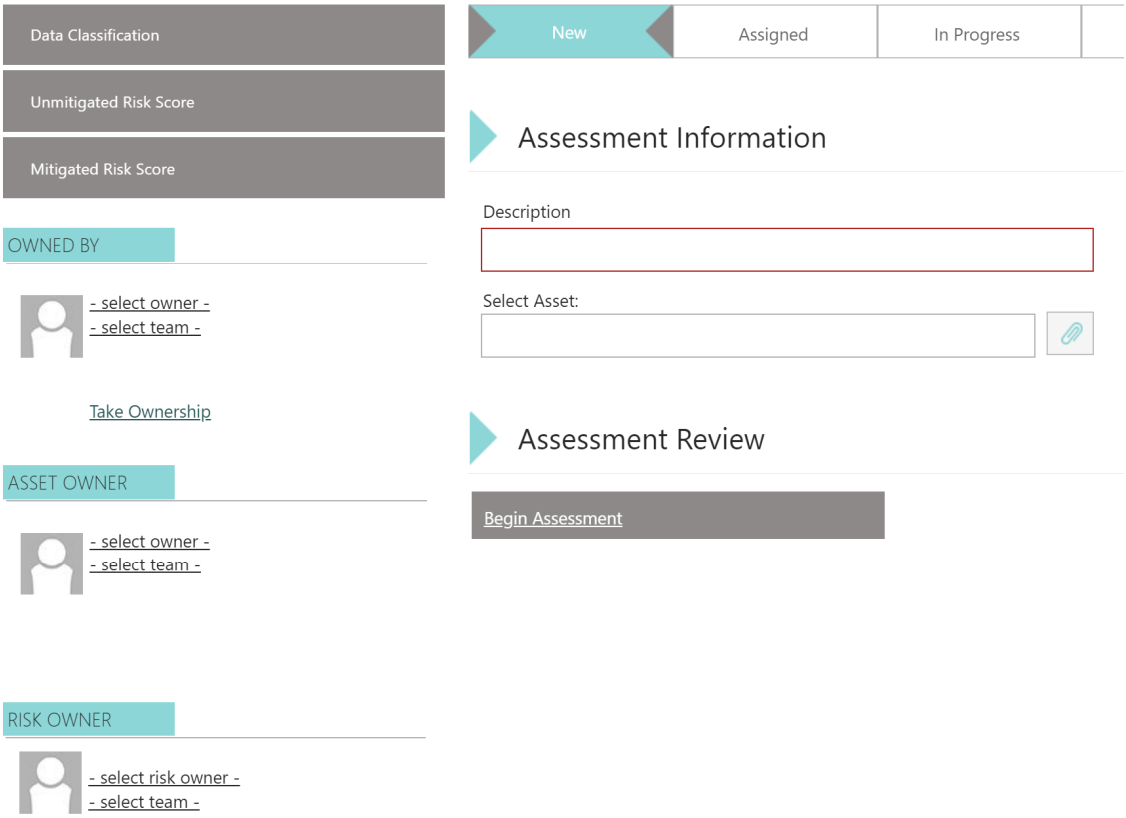


Abbildung 16: Erfassung von Risikobewertungen in CSM

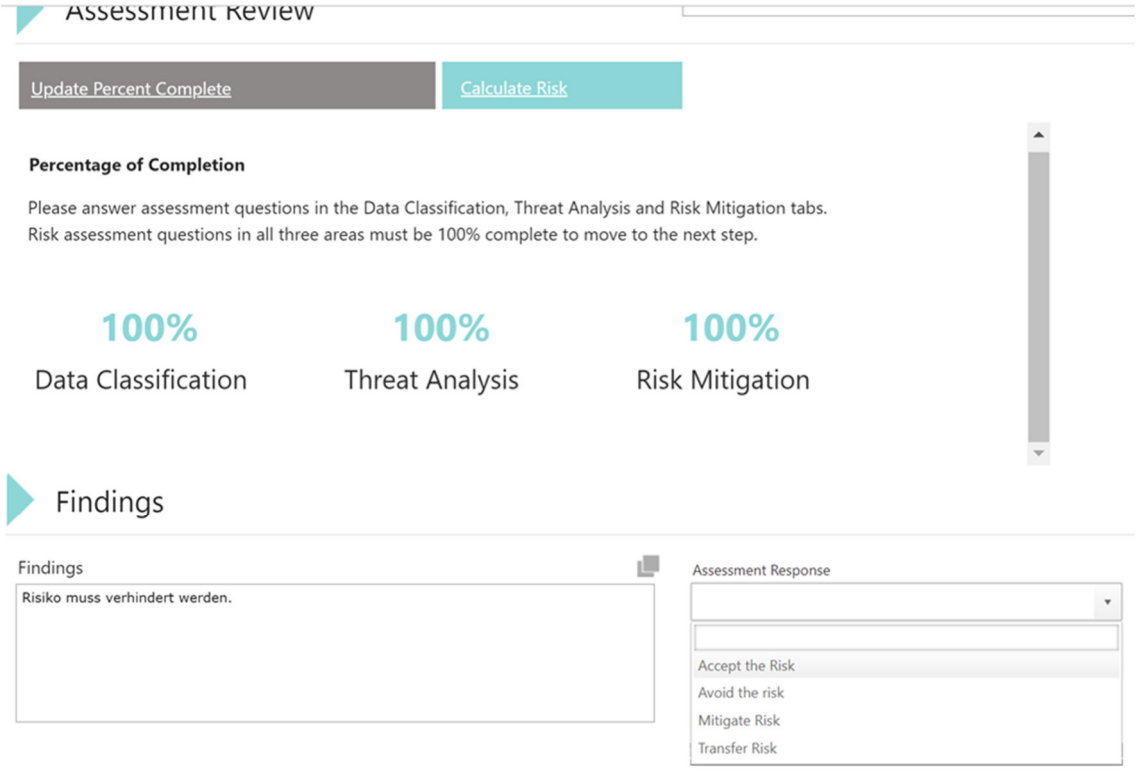


Abbildung 17: Bearbeitung bewerteter Risiken in CSM

Die siebte IT-GRC Funktion von CSM unterstützt die Durchführung von Audits. Diese IT-GRC Funktion erfasst zuerst die Details des Audits (vgl. Abbildung 17). Anschliessend werden der Lead Auditor und die Teilnehmenden mit dem zu erfassenden Audit verknüpft. Es folgt die Definition des Auditumfangs und -zeitplans. Der erfasste Audit wird zur Genehmigung aufgegeben. Weiter ermöglicht CSM die Verknüpfung von Security Incidents, Risikobewertungen und Steuerelementen. Die Ergebnisse des Audits und allfällige Massnahmen werden dokumentiert. Damit wird der Audit abgeschlossen. CSM bietet ein IT-GRC Dashboard an, welches Informationen zu Objekten des Moduls ISMS visualisiert. Neben den bereits genannten Objekten, mit denen die sieben IT-GRC Funktionen von CSM interagieren, behandelt das Modul ISMS zusätzlich Security Events und Security Incidents.

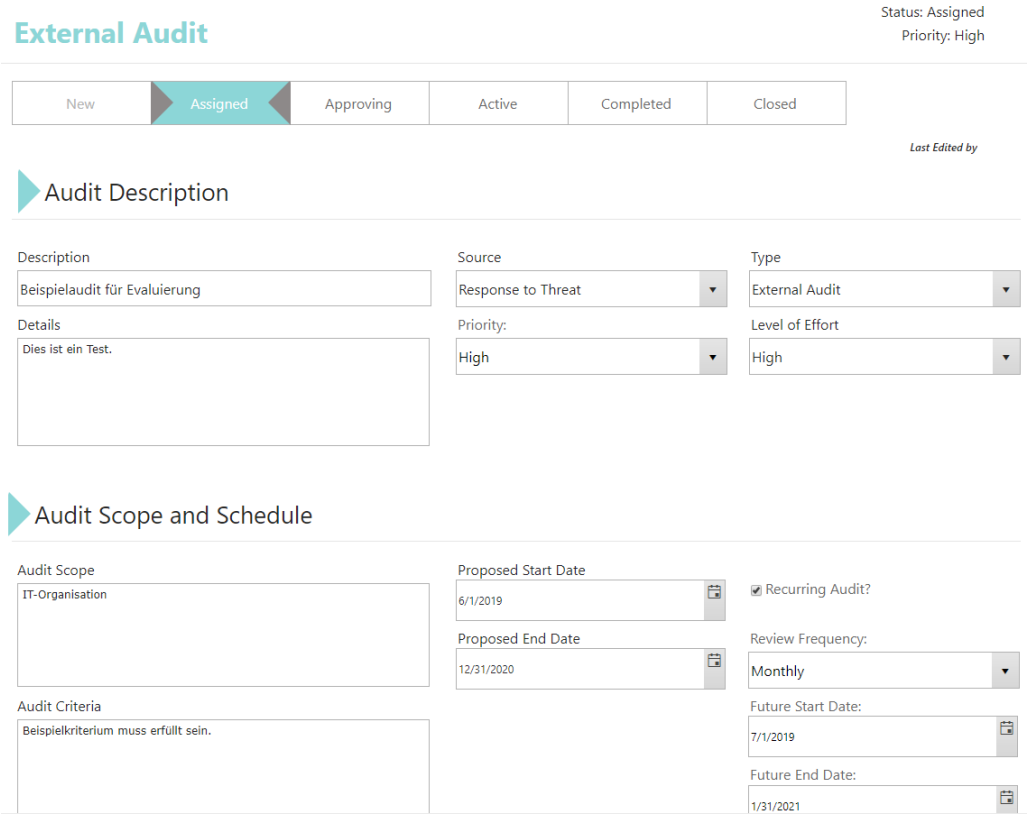


Abbildung 18: Erfassung von Audits in CSM

Im IT-GRC Dashboard werden die Anzahl der Security Incidents und deren Priorität abgebildet. Weiter sind die Informationen zu aktiven Regelwerken, internen Vorgaben, offenen Audits, präventiven oder korrektiven Massnahmen, externen Vorgaben und Risiken auf einem Blick visualisiert. Mit einem Klick auf eine Abbildung öffnen sich die Datensätze des ausgewählten Objekts. Wird ein Datensatz ausgewählt, findet ein Absprung auf die zugehörige IT-GRC Funktion statt, wo der Datensatz bearbeitet werden kann.

5.2 Evaluierung der IT-GRC Funktionen von Ivanti

Ivanti dient als zweiter ITSM Lösunganbieter für die Evaluierung der IT-GRC Funktionen in führenden ITSM Lösungen. Ivanti wurde als IT-Unternehmen durch den Zusammenschluss von LANDESK und HEAT im Januar 2017 gegründet (Gonzalez et al., 2018). Die Gründung von LANDESK reicht ins Jahr 1985 zurück, wobei HEAT im Jahr 2015 selbst durch einen Zusammenschluss entstanden ist. Das amerikanische IT-Unternehmen Ivanti hat seinen Sitz in South Jordan, Utah, und bietet Software für IT-Security, ITSM, IT-Asset Management, Unified Endpoint Management, Identity Management und Supply Chain Management an (Bloomberg, 2019b). Die ITSM Lösung von Ivanti wird Ivanti Service Manager (ISM) bezeichnet, welche sich gemäss Gonzalez et al. (2018) effektiv über Kanäle vermarktet hat, die Unternehmen mit geringer bis mittlerer I&O-Reife ansprechen. Die Mehrheit der Kunden nutzt die Dienste von Ivanti jedoch On-Premises anstelle von Cloud, obwohl Optionen für Cloudlösungen vorhanden sind (Gonzalez et al., 2018). Durch den Zusammenschluss von LANDESK und HEAT wurden gemäss Gonzalez et al. (2018) Möglichkeiten für die Kunden geschaffen, auf die aktuelle Plattform zu migrieren. Aus diesem Grund klassifiziert sich Ivanti als führender ITSM Lösungsanbieter. Der Preis von ISM hängt von der Ausbaustufe und dem Modell Cloud oder On-Premise ab. Bei Ivanti wird ausschliesslich über die Zahl der Analysten anstelle der Benutzer lizenziert. Die Effizienz sowie Zuverlässigkeit von ISM ist sehr ausgereift und die Usability von ISM hoch zu werten. IT-GRC Funktionen werden in CSM nicht gesondert angeboten, sondern befinden sich in anderweitigen Prozessen integriert und stehen somit im Standard zur Verfügung. In der Produktdokumentation und in der ISM-Testumgebung von Ivanti (2019) lassen sich Funktionen für das Aufgabengebiet von IT-GRC gemäss Kapitel 2.3.2 identifizieren.

Zum einen verwaltet Ivanti (2019) in ISM im Portfolio Management und im Change Management Risiken. So ist in jedem Portfolio ein Tab hinterlegt, wo Risiken gemäss der Abbildung 19 manuell erfasst oder bearbeitet werden können. Neben dem Titel und der Beschreibung des Risikos werden der Typ, der Schweregrad, der Status, der Verantwortliche, die Wahrscheinlichkeit und die Reaktion des Risikos definiert. Als Reaktion stehen das Akzeptieren, Vermeiden, Übertragen oder Verringern des Risikos zur Auswahl. Weiter kann ein Notfallplan hinterlegt, eine Eskalation sowie inbegriffen mit einem Datum und einer Begründung ausgelöst oder eine Verteilerliste über die zu informierenden Personen angegeben werden. Treten Probleme innerhalb des Portfolios auf, werden Risiken mit den Problemen für die Problembehandlung verknüpft.

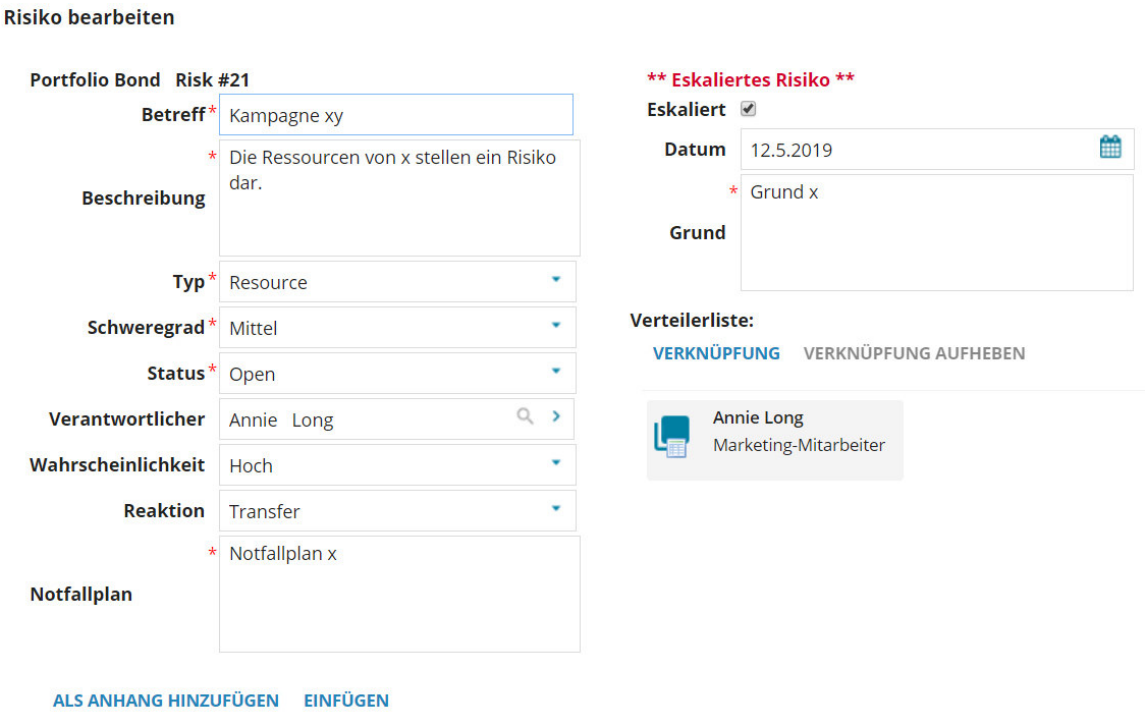


Abbildung 19: Verwaltung von Risiken in ISM

Zum anderen ermöglicht ISM die Risikobewertung von Changes, indem ein konfigurierbarer Fragebogen gemäss der Abbildung 20 beantwortet wird. Die Risikobewertung eines Changes umfasst die Identifizierung von betroffenen Konfigurationselementen und die anschliessende Einschätzung der Auswirkungen auf die IT-Organisation und das Business. Es wird eine Einstufung des Risikos berechnet, um dann über die Risikobehandlung beziehungsweise über die Umsetzung des Changes zu entscheiden.

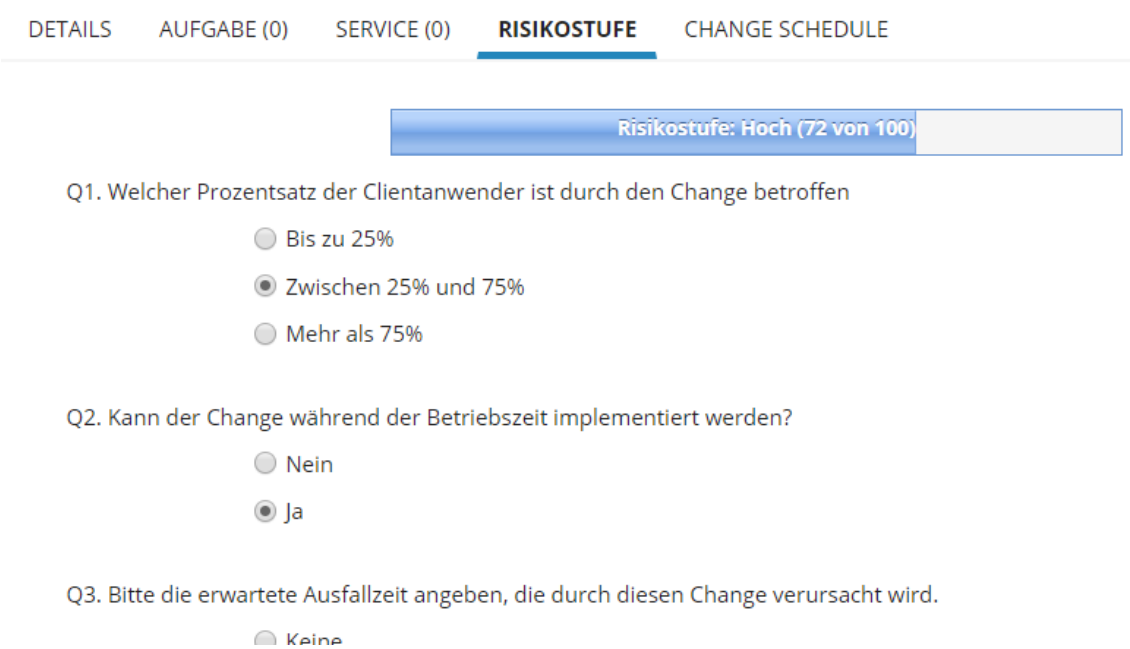


Abbildung 20: Bewertung von Risiken in ISM

Das Service Level Manager Dashboard, welches Ivanti (2019) zur Verfügung stellt, dient gemäss der Abbildung 21 als Werkzeug zur Überwachung der Compliance. In ISM können gemäss Recherchen in der Produktdokumentation von Ivanti (2019) weder interne noch externe Vorgaben definiert werden. Das Service Level Manager Dashboard ermöglicht jedoch, Auskunft über werksseitig definierte Vorgaben zu geben. Die Vorgaben geben in diesem Dashboard Auskunft über den Trend von Serviceanfragen erteilt. Weiter wird ein Vergleich zwischen dem Soll-Zustand und dem Ist-Zustand der SLAs zum einen aus Sicht von Organisationseinheiten und zum anderen aus Sicht von Services gezogen. Auch wird je nach Team die Zielvereinbarung mit der tatsächlichen Einhaltung der einzelnen Vereinbarungen auf operativer Ebene verglichen. Schlussendlich zeigt das Dashboard noch einen Vergleich des Soll-Zustands und des Ist-Zustands der einzelnen Rahmenverträge von Lieferanten.

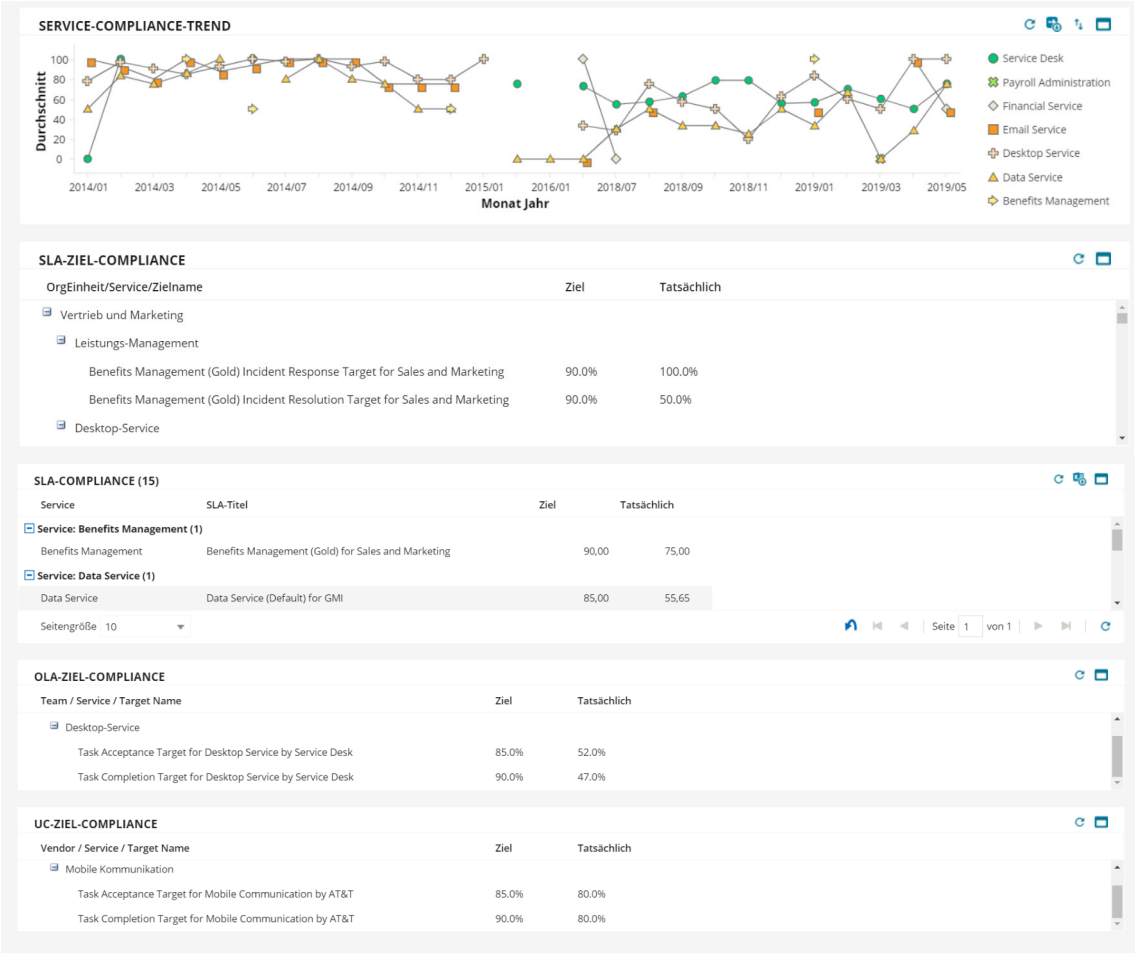


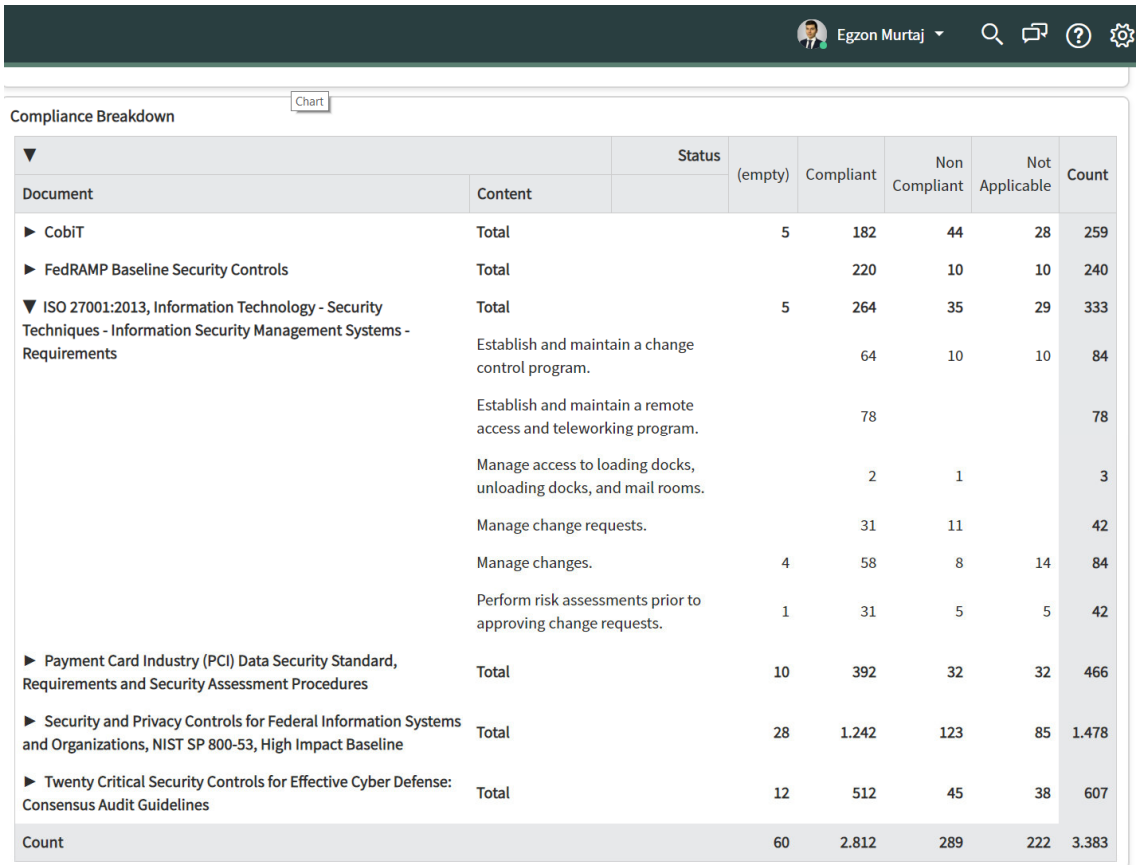
Abbildung 21: Compliance Dashboard in ISM

5.3 Evaluierung der IT-GRC Funktionen von ServiceNow

Für die Evaluierung von IT-GRC Funktionen in führenden ITSM Lösungen wird in der Bachelorarbeit ServiceNow als dritter ITSM Lösungsanbieter selektiert. ServiceNow wurde analog zu Cherwell Software im Jahr 2004 in den USA gegründet, bietet Lösungen zu ITSM sowie digitalen Workflows auf Basis von Cloud Computing an und erwirtschaftete im Jahr 2018 einen Umsatz von über 2,608 Milliarden US-Dollar (Bloomberg, 2019c; ServiceNow, 2019a). Die Lösungen von ServiceNow adressieren nicht nur IT-Organisationen, sondern unter anderem auch Kundenservices oder Personalabteilungen (Bloomberg, 2019c). Die ITSM Lösung von ServiceNow namens ServiceNow ITSM richtet sich an Unternehmen mit unterschiedlichen I&O-Reifegraden (Gonzalez et al., 2018). Aufgrund eines globalen Vertriebsnetzes und einer Markenbekanntheit dominiert ServiceNow ITSM den Markt für ITSM Lösungen (Gonzalez et al., 2018). Der Sitz von ServiceNow befindet sich in Santa Clara, Kalifornien (Bloomberg, 2019c). In ServiceNow ITSM sind IT-GRC Funktionen nicht im Standard enthalten. Die IT-GRC Funktionen stehen jedoch modular als Plugins zur Verfügung, die im ServiceNow Store der ITSM Lösung abrufbar sind. Die für den Kunden anfallenden Lizenzkosten für die Nutzung von ServiceNow ITSM und der IT-GRC Funktionen sind je nach Kunden flexibel gestaltet. Bei ServiceNow ISTM lässt sich in der Evaluierung eine sehr hohe Effizienz, Usability und Zuverlässigkeit feststellen. Konkret dienen in der ITSM Lösung von ServiceNow (2019b) ein Policy and Compliance Management, Risk Management, Audit Management und Vendor Risk Management als IT-GRC Funktionen, die einzeln und voneinander unabhängig installiert werden können.

Das Policy and Compliance Management in ServiceNow ITSM umfasst die Verwaltung von Vorgaben, Ausnahmeregelungen, Steuerelementen, Compliance Problemen und vom Monitoring. Das Policy and Compliance Management ermöglicht zum einen das Erstellen, Beurteilen, Genehmigen, Veröffentlichen und Zurückziehen von Richtlinien, anhand welcher interne Vorgaben erstellt werden. Zum anderen wird das Erfassen von externen Vorgaben unterstützt, welche aus Regelwerken gemäss der Abbildung 22 abgeleitet werden können. Regelwerke werden vom Unified Compliance Framework (UCF) heruntergeladen. Der UCF bildet eine Plattform von Regelwerken, welcher von ServiceNow gepflegt und zur Verfügung gestellt wird. Externe Vorgaben können jedoch auch manuell erstellt werden. Bei Ausnahmeregelungen besteht ein Workflow, der das Beantragen, Genehmigen und Protokollieren von vorübergehenden Ausnahmeregelungen ermöglicht. Durch die Relation von Ausnahmeregelungen und Vorgaben werden die betroffenen

Steuerelemente identifiziert und im Antrag gelistet. Anträge zu Ausnahmeregelungen werden von Verantwortlichen entweder akzeptiert oder abgelehnt. Als zusätzliche Funktion können für unklare Entscheidungen Risiko-Verantwortliche beigezogen werden, die eine Risikobewertung zu Ausnahmeregelungen durchführen. Anhand der Risikobewertungen wird eine weitere Grundlage für das Akzeptieren oder das Ablehnen der Ausnahmeregelungen gebildet. Die Verwaltung von Steuerelementen schliesst das Erstellen, Verfolgen und Attestieren von Steuerelementen ein. Die Attestierung von Steuerelementen weist nach, wie erfolgreich Steuerelemente umgesetzt wurden. Weiter können Indikatoren angelegt werden, um Daten periodisch sowie automatisiert zu erheben. Eine automatisierte Erfassung von Problemen tritt auf, sobald ein solcher Indikator die Grenzwerte übersteigt, eine negative Attestierung aus einem Steuerelement resultiert oder eine Prüfung eines Steuerelements fehlschlägt. Das Monitoring der Compliance basiert auf konfigurierbare Dashboards, welche Auskunft zum Stand der Compliance über Datenvisualisierungen ausgeben.



Document	Content	Status	(empty)	Compliant	Non Compliant	Not Applicable	Count
► CobiT	Total		5	182	44	28	259
► FedRAMP Baseline Security Controls	Total			220	10	10	240
▼ ISO 27001:2013, Information Technology - Security Techniques - Information Security Management Systems - Requirements	Total		5	264	35	29	333
	Establish and maintain a change control program.			64	10	10	84
	Establish and maintain a remote access and teleworking program.			78			78
	Manage access to loading docks, unloading docks, and mail rooms.			2	1		3
	Manage change requests.			31	11		42
	Manage changes.		4	58	8	14	84
	Perform risk assessments prior to approving change requests.		1	31	5	5	42
► Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures	Total		10	392	32	32	466
► Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53, High Impact Baseline	Total		28	1.242	123	85	1.478
► Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines	Total		12	512	45	38	607
Count			60	2.812	289	222	3.383

Abbildung 22: Auflistung erfasster Regelwerke in ServiceNow ITSM

Das Risk Management in ServiceNow ITSM verwaltet zum einen Risiken, Risk Statements sowie Risk Frameworks und zum anderen Risikobewertungen. Weiter sind analog zum Policy and Compliance Management die Problembehandlung und das Monitoring der Risiken enthalten. Risk Frameworks und Risk Statements können erstellt werden, wobei Risiko Frameworks aus Risk Statements bestehen und damit die Risikopraktiken des Unternehmens gemäss der Abbildung 23 festhalten. Anhand der Risk Frameworks sowie der Risk Statements lassen sich Risiken ableiten. Risiken werden anhand von Indikatoren gemessen und weiteren Risiken zugeordnet, um die Bearbeitungen zu bündeln. Neben Indikatoren messen auch zugewiesene Steuerelemente ein Risiko. Zusätzlich besteht die Möglichkeit, RiskLens als Provider für Risikoanalysen in das Risk Management in ServiceNow ITSM zu integrieren und deren Dienste in Anspruch zu nehmen. Weiter ist im Risk Management eine Risikobewertung mit dem Erstellen und Bearbeiten von Attestierungen sowie Bewertungsparametern möglich. In der Risikobewertung werden Risikodaten gesammelt, um daraus die Risikoakzeptanz zu bestimmen. Eine von ServiceNow zur Verfügung gestellte Bibliothek bietet Fragen zu verschiedenen Kategorien an, die für eigene Fragebogen adaptiert werden können, um die Risikobewertung durchzuführen. Analog zum Policy and Compliance Management können Probleme automatisiert oder manuell erfasst werden. Das Vendor Risk Management in ServiceNow ITSM bearbeitet die Risiken von Lieferanten, wird jedoch in einem eigenen Plugin angeboten. Das Vendor Risk Management zentralisiert die Verwaltung des Lieferantenportfolios sowie die Bewertung und die Einstufung des Lieferantenrisikos.

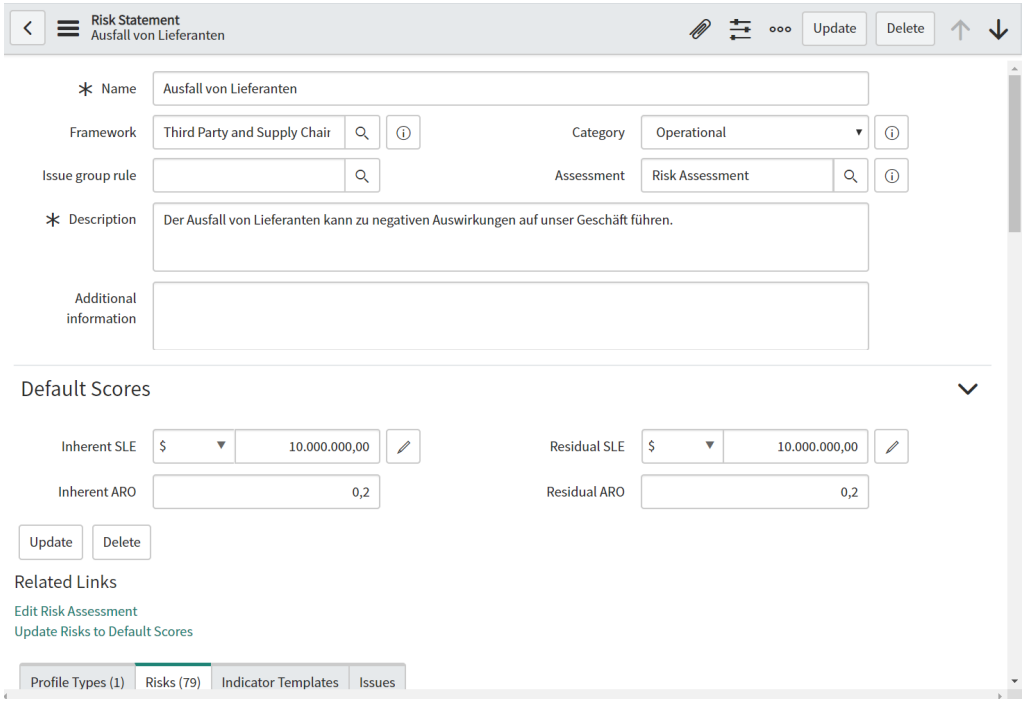


Abbildung 23: Risk Statement in ServiceNow ITSM

Das Audit Management in ServiceNow ITSM automatisiert Audittätigkeiten auf Grundlage von Steuerelementen des Policy and Compliance Managements und Risk Managements. Die zu automatisierenden Audittätigkeiten betreffen die Planung, die Durchführung und die Berichterstattung von Audits. Für die Planung von Audits werden Prüfvorlagen und -pläne hinterlegt, wobei Prüfvorlagen mit Vorgaben verknüpft werden können. Für die Durchführung von Audits wird ein Engagement, eine Prüfung eines Steuerelements, eine Aktivität, ein Interview, eine Anleitung oder ein Knowledge Base Artikel erfasst. Beispielsweise können gemäss der Abbildung 24 alle erfassten Engagements überwacht werden. Die Ergebnisse der Indikatoren werden verwendet, um automatisiert Probleme zu erfassen, die Risikobewertung zu aktualisieren und unterstützende Informationen für die Auditaktivitäten und Prüfung von Steuerelementen bereitzustellen. Nach der Durchführung von Audits können zuvor erstellte Berichtsvorlagen genutzt werden. Die Berichterstattung von Audits informiert die betroffenen Anspruchsgruppen über die Ergebnisse der Audits.

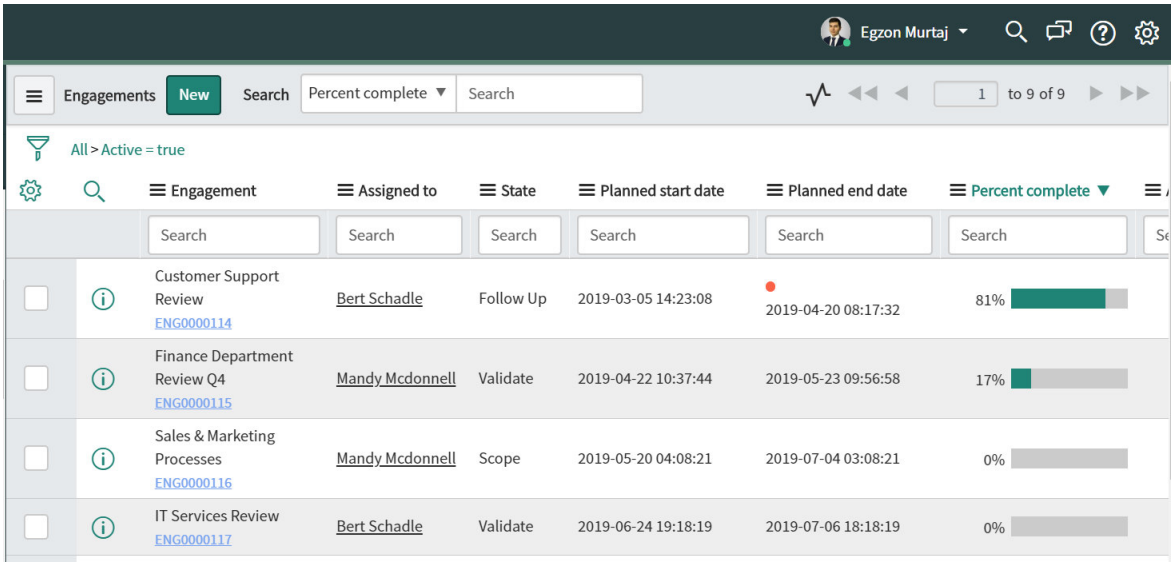


Abbildung 24: Audit Engagements in ServiceNow ITSM

6 Beurteilung der Forschungserkenntnisse

Dieses Kapitel beurteilt den Einsatz von IT-GRC Funktionen in ITSM Lösungen. Es werden Punkte für die drei führenden ITSM Lösungen anhand des Bewertungskatalogs und der Evaluierung vergeben, woraus eine Nutzwertgewichtung entsteht. Nach der Nutzwertgewichtung soll dargelegt werden, welche Mächtigkeit IT-GRC Funktionen in ITSM Lösungen aufweisen und somit welche Möglichkeiten sich für IT-Organisationen ergeben. Es folgt eine kritische Betrachtung über die Limitation, unter anderem ob angepriesene IT-GRC Funktionen realitätstauglich sind und welche Grenzen zum Anwendungsgebiet von IT-GRC Funktionen in ITSM Lösungen bestehen.

6.1 Nutzwertgewichtung der führenden ITSM Lösungen

Anhand des Bewertungskatalogs vom Kapitel 4 und der Evaluierung vom Kapitel 5 wird wird die Nutzwertgewichtung der führenden ITSM Lösungen in Bezug auf IT-GRC Funktionen in der Tabelle 5 aufgezeigt. Wie bereits aus dem Bewertungskatalog entnommen werden kann, repräsentiert 5 die höchste und 1 die niedrigste Bewertung.

					Cherwell Software		**Ivanti**		**ServiceNow**	
			Kriterien	Gewichtung	Punkte	Nutzwert	Punkte	Nutzwert	Punkte	Nutzwert
Funktionale Kriterien	Risk Management	R1	Definition des Risikoappetits		3		1		4	
		R2	Verwaltung von Risikopraktiken		5		3		5	
		R3	Bewertung von Risiken		4		3		5	
		R4	Monitoring der Risiken		4		3		5	
		R5	Auditabdeckung		5		3		5	
	Compliance Management	C1	Verwaltung von Vorgaben		4		2		5	
		C2	Regelung der Verantwortlichkeiten		4		2		4	
		C3	Überprüfung der Vorgabenverwaltung		4		3		5	
		C4	Monitoring der Compliance		4		2		5	
		C5	Ausnahmeregelung		5		1		5	
Nicht-funktionale Kriterien		N1	Effizienz		5		5		5	
		N2	Usability		3		4		5	
		N3	Zuverlässigkeit		3		4		5	
		N4	ITSM Lösungsanbieter		4		3		5	
		N5	Lizenzierungsmodell		3		5		2	
			Nutzwertsumme							

Tabelle 5: Nutzwertgewichtung führender ITSM Lösungen zu IT-GRC Funktionen

Auf Grundlage der Nutzwertgewichtung gemäss Tabelle 5 zeigt sich im Vergleich, dass die ITSM Lösung von ServiceNow vom Umfang und von der Qualität führend ist. Dicht gefolgt wird ServiceNow von der ITSM Lösung von Cherwell Software. Bei der ITSM Lösung von Ivanti besteht ein erhöhter Nachholbedarf beziehungsweise Verbesserungspotenzial für IT-GRC Funktionen. Die Ergebnisse können auch darauf zurückgeführt werden, dass ServiceNow die IT-GRC Funktionen in einem gesonderten Modul anbietet und im Vergleich zu den anderen ITSM Lösungsanbietern am höchsten anpreist. Cherwell Software setzt die IT-GRC Funktionen mit jenen der IT-Security in einem gemeinsamen Modul zusammen und bei Ivanti sind die IT-GRC Funktionen in keinem Modul vorhanden, sondern in verschiedenen Prozessen der ITSM Lösung integriert. Auf den ersten Blick konnten bei der ITSM Lösung von Ivanti keine IT-GRC Funktionen identifiziert werden. Erst nach umfassenden Recherchen in der Produktdokumentation wurden IT-GRC Funktionen erkannt. Obwohl die ITSM Lösung von ServiceNow führend in IT-GRC Funktionen ist, bestehen auch bei ihr Verbesserungspotenziale. So können in Zukunft beispielsweise IT-GRC Funktionen implementiert werden, welche eine Segregation of Duties in der ITSM Lösung von ServiceNow ermöglichen.

6.2 Mächtigkeit und Limitation

Wie die Evaluierung gemäss Kapitel 5 aufgezeigt hat, weisen die ITSM Lösungsanbieter Stärken und Schwächen auf, woraus die Mächtigkeit und Limitation von IT-GRC Funktionen in ITSM Lösungen abgeleitet werden kann.

Der Einsatz von IT-GRC Funktionen in ITSM Lösungen weist eine unterschiedliche Mächtigkeit vor. Gemäss der Experteninterviews besteht ein Aspekt der Mächtigkeit darin, dass ITSM Lösungen den gesamten Lebenszyklus eines IT-Service abdecken, das Zusammenspiel mit IT-GRC auf unterschiedlichen Ebenen stattfinden kann und abgeleitet die Effektivität, die Effizienz und das ethische Verhalten von IT-Services positiv beeinflusst wird. Im Rahmen der Prozessumsetzung werden zum Beispiel Kennzahlen oder ausgeführte Kontrollen an Governance Bodies gemeldet, wodurch Management Impulse entstehen können. ITSM Lösungen mit integrierten IT-GRC Funktionen ermöglichen somit, die zwei Welten IT-GRC und ITSM miteinander zu verbinden. Unter anderem kann in der ITSM Lösung eine Vorgabe definiert werden, wie mit Changes umzugehen ist. Die Überprüfung der Vorgabe kann automatisiert erfolgen, sobald die Changes mit der Vorgabe verknüpft sind. Automatisierte Prüfungen umfassen beispielsweise die Fragen, ob Changes autorisiert sind, ob eine Planung vorliegt, ob die Verantwortlichkeiten geklärt

sind oder ob die verantwortlichen Personen überhaupt noch im Unternehmen tätig sind. Je zentraler die Aufgaben des Risk Managements und des Compliance Managements verwaltet werden, umso eher ist gemäss der Experteninterviews die Wahrscheinlichkeit, die Qualität der Services positiv zu beeinflussen.

Unter anderem besteht die Mächtigkeit im Einsatz von IT-GRC Funktionen in ITSM Lösungen auch darin, das Continual Service Improvement positiv zu beeinflussen. Zum Beispiel kann eine Vorgabe definiert werden, Dokumentationen im Vier-Augen-Prinzip zu überprüfen. Dokumentationen, die keiner Überprüfung unterlegen sind, besitzen gemäss der Experteninterviews eine niedrigere Qualität als jene Dokumentationen, die einer Überprüfung unterzogen werden. Mit IT-GRC kann eine automatisierte Rückkopplung der Dokumentationen errichtet werden. Beispielsweise werden vom operativen Change Management monatliche Kontrollhandlung auf Basis der Dokumentationen durchgeführt. Die Kontrollhandlungen überprüfen automatisiert, ob die Dokumentationen den Vorgaben entsprechen. Bei abweichenden Fällen sind korrigierende Massnahmen definiert, wobei diese korrigierenden Massnahmen wiederum für sich einer Kontrolle unterlegen sind.

Gemäss der Experteninterviews bildet die Geschwindigkeit einen weiteren, zentralen Aspekt der Mächtigkeit. Die Geschwindigkeit von Prozessen kann durch IT-GRC Funktionen erhöht werden, indem beispielsweise Nachweise über die aktuelle Einhaltung aller Vorgaben und über die aktuelle Überwachung aller Risiken innert kürzester Zeit der Revision vorgelegt werden können. Klassische Interviews zur Erhebung von revisionsbezogenen Daten, die mit bedeutend höherem Aufwand und damit Kosten verbunden sind, werden obsolet. Dieses Beispiel zeigt auf, dass auch die Mächtigkeit darin besteht, langfristig eine Senkung des Aufwands und damit der Kosten zu erzielen.

Damit Unternehmen überhaupt von den Möglichkeiten profitieren können, muss eine führende ITSM Lösung in der IT-Organisation etabliert und die für die IT-GRC Funktionen betroffenen Daten miteinander verknüpft sein. Mit dieser Anforderung zeigt sich der erste Aspekt der Limitation zum Einsatz von IT-GRC Funktionen in ITSM Lösungen. IT-Organisationen, die keine führende ITSM Lösung mit IT-GRC Funktionen nutzen, müssen mit initial hohen Aufwänden und Kosten rechnen. Zuerst muss die IT-Organisation eine auf die Bedürfnisse abgestimmte ITSM Lösungen beschaffen, da gemäss der Experteninterviews die Bedürfnisse von der Branche und der Grösse des Unternehmens abhängen. Anschliessend müssen die internen Prozesse auf die ausgewählte ITSM Lösung

umgestellt werden, womit erst in diesem Schritt der Grundstein für den Einsatz von IT-GRC Funktionen in ITSM Lösungen gelegt wird. Da der initiale Aufwand gemäss der Experteninterviews enorm ist, zeigt sich eher für Grossunternehmen ein Mehrwert zum Einsatz von IT-GRC Funktionen in ITSM Lösungen. Schlanke ITSM Lösungen, die eher für kleinere Unternehmen vom Aufwand und damit vom finanziellen Aspekt zu bewältigen sind, bieten nach Recherchen keine ausgeprägten IT-GRC Funktionen an.

Die Grenzen beim Einsatz von IT-GRC Funktionen in ITSM Lösungen liegen gemäss der Experteninterviews auch im Detaillierungsgrad und der enorm zunehmenden Komplexität. Das Problem besteht darin, wie weit ITSM Lösungsanbieter ins Detail von IT-GRC Funktionen gehen wollen und können, da die Ressourcen dazu begrenzt sind. Entsprechend werden IT-GRC Funktionen hauptsächlich nur von führenden ITSM Lösungen angeboten. Je nach Plattform der ITSM Lösung belaufen sich gemäss der Experteninterviews die Grenze des gebotenen Funktionsumgangs dort, wo der ITSM Lösungsanbieter keine Unterstützung mehr anbieten kann oder die Kriterien der Anpassbarkeit und Flexibilität nicht gegeben sind.

Ein weiterer Aspekt der Limitation besteht darin, dass automatisierte Messungen zurzeit nur in Prozessen möglich sind, die von IT-Organisationen in der ITSM Lösungen abgebildet und aktiv genutzt werden. Prozesse, die entweder von der IT-Organisation nicht in die ITSM Lösungen integriert wurden oder dies seitens der ITSM Lösungen nicht ermöglicht wird, bleiben der automatisierten Überwachung. In diesem Zusammenhang besteht jedoch das Potenzial, dass die automatisierte Überwachung ausserhalb der aktuellen ITSM Lösungen expandiert. ITSM Lösungsanbieter expandieren immer mehr in Prozesse ausserhalb der IT-Organisation, weshalb stetig weitere Services ausserhalb der IT-Organisation wie beispielsweise jener der Finanzbuchhaltung oder der Personalabteilung von den ITSM Lösungsanbietern abgedeckt werden. Gemäss der Experteninterviews wandeln sich die führenden ITSM Lösungen zu ESM Lösungen, was den Einfluss von IT-GRC Funktionen in ITSM Lösungen beziehungsweise in ESM Lösungen vergrössern könnte.

7 Schlussfolgerung

Dieses Kapitel bietet eine Schlussfolgerung der Bachelorarbeit, indem unter Zuhilfenahme der Forschungsfragen die Ergebnisse der Bachelorarbeit zusammengefasst werden und eine Handlungsempfehlung erstellt wird. In der ersten Teilfrage wurden die theoretischen Grundlagen durchleuchtet, welche Berührungspunkte ITSM und IT-GRC aufweisen. ITSM knüpft an das Zielkonflikt zwischen der Qualitäts- und Aufwandsanforderungen an die IT-Organisation und strebt die Stärkung der Kundenorientierung, die Optimierung der Kostenkontrolle und weitere Nutzenpotenziale für IT-Services durch das Zusammenführen von Prozessmanagement und branchenspezifischen Best Practices an (Rouhani, 2017, S. 730). Für ITSM hat sich ITIL V3 2011 branchenübergreifend etabliert und ist gefolgt von COBIT 5 das Framework mit der weltweit höchsten Akzeptanzrate in IT-Organisationen (Marrone & Kolbe, 2011, S. 5 f.). ITIL V3 2011 interpretiert die IT nicht nur als Technologie, sondern als Mittel zur Erbringung von Services für Kunden. Während der Erarbeitung der Bachelorarbeit ist die neuere Version von ITIL namens ITIL 4 erschienen, welche umso mehr versucht, Silos in IT-Organisationen aufzubrechen. IT-GRC ist immer öfters in IT-Organisationen anzutreffen, da mit der gleichzeitigen Ausbreitung der Digitalisierung von Geschäftsprozessen und der steigenden Komplexität auch die Nachfrage an IT-GRC steigt. Grosse Unternehmen setzen die IT nicht nur zur Unterstützung des Geschäfts, sondern teilweise auch als Business Enabler und Innovator ein, um überhaupt Geschäftstätigkeiten zu ermöglichen (Albayrak & Gadatsch, 2017, S. 154). IT-GRC fungiert zwischen dem unternehmensübergreifendem GRC und der IT, bei welcher unter anderem mit der Governance eine IT-Organisation an die Unternehmensziele ausgerichtet, mit dem Risk-Management mögliche Gefahren behandelt und mit der Compliance die Vorgabeneinhaltung gesichert werden sollen. Für das Anwendungsgebiet von IT-GRC bietet sich COBIT 5 als Framework an (Andelfinger & Kneuper, 2017, S. 27). Auch für COBIT wurde eine neuere Version mit der Bezeichnung COBIT 2019 veröffentlicht, welche eine höhere Akzeptanz und Umsetzbarkeit in Unternehmen anvisiert (ISACA, 2018). Da zwischen ITIL V3 2011 und COBIT 5 Überschneidungen bestehen, sind auch zwischen ITSM und IT-GRC Überschneidungen anzutreffen. ITSM dient IT-GRC zum einen als Bewertungsobjekt und zum anderen als Werkzeug, indem IT-GRC relevante Aufgaben funktional in ITSM Lösungen abgebildet werden. Konkret handelt es sich gemäss der Experteninterviews um die Aufgaben des Risk Managements und Compliance Managements, die über IT-GRC Funktionen gemäss der Abbildung 11 in ITSM Lösungen unterstützt werden können.

Für die zweite Teilfrage wurden die führenden ITSM Lösungen identifiziert, welche am Markt angeboten werden. Pröhl & Zarnekow (2019) beschreiben den Markt von ITSM Lösungen als vielfältig und voluminös. Die ITSM Lösungsanbieter unterscheiden sich gemäss der Experteninterviews voneinander, indem einzelne, kleinere ITSM Lösungsanbieter sich auf einzelne Themen spezialisieren und Marktnischen für sich beanspruchen, wobei führende ITSM Lösungsanbieter wiederum möglichst das ganze Spektrum der IT-Organisation abdecken. Gonzalez et al. (2018) vom IT-Beratungsunternehmen Gartner ernennen Axios Systems, BMC Software, CA Technologies, Cherwell Software, EasyVista, IBM, Ivanti, Micro Focus und ServiceNow als führende ITSM Lösungsanbieter. Analog zu Gonzalez et al. (2018) zählen Betz et al. (2018) vom Unternehmen Forrester Research die ITSM Lösungen von Atlassian, Axios, BMC Software, CA Technologies, Cherwell Software, EasyVista, IBM, Ivanti, Micro Focus, ServiceNow, SunView und TOPdesk als führend auf. BMC Software und ServiceNow werden von Gonzalez et al. (2018) als Leader spezifiziert, wobei Cherwell Software und Ivanti als Challenger eingestuft werden, die an der Grenze zur Kategorie Leader stehen. Betz et al. (2018) klassifizieren ServiceNow und Cherwell Software als Leader sowie BMC Software und Ivanti als Strong Performer. Für die spätere Evaluierung werden die ITSM Lösungen von Cherwell Software, Ivanti und ServiceNow selektiert.

Zur Beantwortung der dritten Teilfrage wurden die Bewertungskriterien in einem Bewertungskatalog ernannt, die den Einsatz von IT-GRC Funktionen in ITSM Lösungen messen. Die Bewertungskriterien sind in funktionale und nicht-funktionale Kriterien unterteilt. Funktionale Kriterien bewerten die Unterstützung der Funktionen für das Aufgabengebiet, für welches es konzipiert wurde, wobei nicht-funktionalen Kriterien sich auf die Qualitätsmerkmale der angebotenen Funktionen beziehen (Rouhani & Ravasan, 2014, S. 7 ff.). Als funktionale Kriterien, die in der Kategorie *Risk Management* angesiedelt sind, werden die Definition des Risikoappetits, die Verwaltung von Risikopraktiken, die Bewertung von Risiken, das Monitoring der Risiken und die Auditabdeckung genannt. Als funktionale Kriterien in der Kategorie *Compliance Management* gelten die Verwaltung von Vorgaben, die Regelung der Verantwortlichkeiten, die Überprüfungen der Vorgabenverwaltung, das Monitoring der Compliance und die Ausnahmeregelung. Da der Fokus der Bachelorarbeit in der Evaluierung von Funktionen liegt, werden nur die relevantesten nicht-funktionalen Kriterien evaluiert, welche sich aus der Effizienz, der Usability, der Zuverlässigkeit, dem ITSM Lösungsanbieter und dem Lizenzierungsmodell zusammensetzen.

Für die vierte Teilfrage wurde eine Evaluierung der ITSM Lösungen von Cherwell Software, Ivanti und ServiceNow auf Grundlage der Bewertungskriterien durchgeführt. Aus der Evaluierung geht unter anderem hervor, dass interne und externe Vorgaben erfasst und kontrolliert werden können. Um die externen Vorgaben nicht manuell zu erfassen, können beispielsweise bei der ITSM Lösung von ServiceNow externe Vorgaben aus Regelwerken abgeleitet werden. Regelwerke werden zentral von ServiceNow gepflegt und den Kunden zur Verfügung gestellt. Weiter werden temporäre Ausnahmeregelungen nach einem Genehmigungsprozess dokumentiert und Risiken innerhalb einer Risikobewertungen behandelt. Eine weitere Rolle spielen Dashboards oder exportierbare Berichte zur Überwachung der IT-GRC. Sowohl in der Qualität als auch in der Quantität führt die ITSM Lösung von ServiceNow im Einsatz von IT-GRC Funktionen. Auch die ITSM Lösung von Cherwell Software bietet umfassende IT-GRC Funktionen, weshalb Cherwell Software als grösste Konkurrenz für die ITSM Lösung von ServiceNow fungiert. Hingegen sind die IT-GRC Funktionen von Ivanti nicht umfassend umgesetzt, weshalb Verbesserungspotenziale bestehen.

Für die fünfte Teilfrage wurden die Forschungserkenntnisse beurteilt, um abschliessend die zentrale Forschungsfrage zu beantworten, welche Möglichkeiten und Grenzen zum Einsatz von IT-GRC Funktionen in führenden ITSM Lösungen bestehen. Gemäss der Experteninterviews besteht die erste zentrale Möglichkeit darin, dass ITSM Lösungen den gesamten Lebenszyklus eines Service abdecken, das Zusammenspiel mit IT-GRC auf unterschiedlichen Ebenen stattfindet und abgeleitet die Effektivität, die Effizienz und das ethische Verhalten von IT-Services positiv beeinflusst wird. Vor allem besteht die Möglichkeit bei der Erzielung von Qualitätsverbesserungen. In den Experteninterviews wird das Beispiel genannt, dass mit IT-GRC Funktionen eine automatisierte Rückkopplung der Dokumentationen errichtet wird. Auf Basis der Dokumentationen vom operativen Change Management werden monatliche Kontrollhandlung durchgeführt, welche automatisiert überprüfen, ob die Dokumentationen den Vorgaben entsprechen und damit die Qualität eingehalten wird. Gemäss der Experteninterviews bildet die Geschwindigkeit eine weitere zentrale Möglichkeit zum Einsatz von IT-GRC Funktionen in führenden ITSM Lösungen. Eine aktuelle Einhaltung aller Vorgaben und eine Übersicht aller Risiken kann innert kürzester Zeit nachgewiesen werden, weshalb manuelle Tätigkeiten reduziert oder gänzlich obsolet werden. Damit IT-Organisationen überhaupt von den Möglichkeiten profitieren können, die aus dem Einsatz von IT-GRC Funktionen in ITSM Lösungen resultieren, muss eine führende ITSM Lösung in der IT-Organisation integriert

sein. Fehlt eine führende ITSM Lösung mit IT-GRC Funktionen, bilden die initial hohen Aufwänden und Kosten die erste zentrale Grenze. Eine weitere zentrale Grenze, die in den Experteninterviews genannt wurde, ist die rasch zunehmende Komplexität im Detaillierungsgrad. Je detaillierter und umfassender IT-GRC Funktionen angeboten werden, desto höher ist die Komplexität und damit der Ressourcenanspruch für den ITSM Lösungsanbieter. Als dritte zentrale Grenze wird genannt, dass automatisierte Messungen zurzeit nur in Prozessen möglich sind, die vom Kunden in der ITSM Lösungen abgebildet und aktiv genutzt werden. Prozesse, die vom ITSM Lösungsanbieter nicht abgebildet und damit nicht angeboten werden, bleiben der automatisierten Messung fern. Da jedoch immer mehr ITSM Lösungen der Rolle als ESM Lösung nacheifern, besteht Potenzial für die Ausweitung des Einsatzes von IT-GRC Funktionen. In zukünftigen Arbeiten kann aufbauend untersucht werden, welche neuen Möglichkeiten und Grenzen sich beim Einsatz von IT-GRC Funktionen in ESM Lösungen ergeben.

Abschliessend wird in Anbetracht der Bachelorarbeit für Organisationen empfohlen, initial einen Abgleich der genannten Möglichkeiten und Grenzen zum Einsatz von IT-GRC Funktionen in führenden ITSM Lösungen vorzunehmen. Aus dem Abgleich der Möglichkeiten und Grenzen soll eine Gewichtung resultieren, anhand welcher die Nutzwertgewichtung gemäss der Tabelle 5 vervollständigt werden kann und dadurch eine ITSM Lösung als Favorit herausragt. Je grösser und vernetzter die Organisationen sind, umso eher soll eine höhere Gewichtung in funktionale Kriterien ausfallen, da grössere Organisationen am meisten von den Möglichkeiten profitieren können. Bei einer höheren Gewichtung von funktionalen Kriterien stellt sich die ITSM Lösung von ServiceNow als Favorit heraus. ServiceNow bietet umfassende IT-GRC Funktionen und gilt auch in den nichtfunktionalen Kriterien als führend. Die Lizenzierungsthematik könnte jedoch Unternehmen davon abhalten, die ITSM Lösung von ServiceNow als Favorit zu betrachten. Ergibt sich in der Lizenzierungsthematik eine höhere Gewichtung, gilt die ITSM Lösung von Cherwell Software als potenzielle Alternative, welche im Umfang und in der Qualität den IT-GRC Funktionen von ServiceNow am nächsten kommt.

8 Literaturverzeichnis

Albayrak, C. A., & Gadatsch, A. (2017). Digitalisierung für kleinere und mittlere Unternehmen (KMU): Anforderungen an das IT-Management. In M. Knoll & S. Strahringer (Hrsg.), *IT-GRC-Management – Governance, Risk und Compliance: Grundlagen und Anwendungen* (S. 151–166). https://doi.org/10.1007/978-3-658-20059-6_10

Andelfinger, U., & Kneuper, R. (2017). Governance und Compliance von Anfang an wirksam umsetzen. In M. Knoll & S. Strahringer (Hrsg.), *IT-GRC-Management – Governance, Risk und Compliance: Grundlagen und Anwendungen* (S. 25–36). https://doi.org/10.1007/978-3-658-20059-6_2

Arikan, C. (2018). Cyberkriminalität in der Schweiz: Starke Zunahme und neue Bedrohungen durch künstliche Intelligenz. Abgerufen von https://home.kpmg/ch/de/home/medien/medienmitteilungen/2017/05/cyberkriminalitaet-in-der-schweiz.html

Betz, C., McKeon-White, W., Rogers, S., Caldwell, J., & Lynch, D. (2018). *The Forrester Wave™: Enterprise Service Management, Q3 2018*. Abgerufen von https://www.forrester.com/report/The+Forrester+Wave+Enterprise+Service+Management+Q3+2018/-/E-RES141112#

Bloomberg. (2019a). Cherwell Software, LLC.: Private Company Information. Abgerufen von https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=224649091

Bloomberg. (2019b). Ivanti Software, Inc.: Private Company Information. Abgerufen von https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=3018494

Bloomberg. (2019c). ServiceNow, Inc.: Private Company Information. Abgerufen von https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=22967487

BMC Software. (2019). IT Governance: An Introduction - BMC Software. Abgerufen von https://www.bmc.com/guides/itil-it-governance

Böhm, M., Müller, S., Krcmar, H., & Welpe, I. (2018). Auswirkungen der digitalen Transformation auf den Wettbewerb. In G. Oswald & H. Krcmar (Hrsg.), *Digitale Transformation: Fallbeispiele und Branchenanalysen* (S. 35–47). https://doi.org/10.1007/978-3-658-22624-4_4

Brandstätter, M., & Peruzzi, T. (2006). Open-ITIL - ein Ansatz zur Akzeptanz-Verstärkung für den Einsatz von IT-Service Management nach ITIL in Klein- und Mittelunternehmen. *Data Warehousing*.

Cannon, D. (2011). *ITIL Service Strategy: 2011* (2nd edition). London: The Stationery Office.

Cherwell Software. (2019a). (GRC) Governance Risk and Compliance Management | Cherwell. Abgerufen von https://www.cherwell.com/products/security-management/governance-risk-compliance

Cherwell Software. (2019b). Cherwell Information Security Management System Documentation. Abgerufen von https://help.cherwell.com/bundle/csm_service_management_solutions_help_only/page/content/esm_solutions/isms/isms_mapp.html

Disterer, G. (2017). Systematische Differenzierung von IT-Risiken. In M. Knoll & S. Strahringer (Hrsg.), *IT-GRC-Management – Governance, Risk und Compliance: Grundlagen und Anwendungen* (S. 83–96). https://doi.org/10.1007/978-3-658-20059-6_6

Feldges, D. (2018). *Novartis will im Kampf gegen Korruption von Siemens lernen | NZZ*. Abgerufen von https://www.nzz.ch/wirtschaft/novartis-will-im-kampf-gegen-korruption-von-siemens-lernen-ld.1411477

Glenfis AG. (o. J.). *ITIL© Edition 2011 - COBIT® 5 Mapping*. Abgerufen von https://www.glenfis.ch/application/files/1814/3040/2298/ITIL_Edition_2011_-_COBIT_5_-Mapping-22.pdf

Gonzalez, K., Doheny, R., & Matchett, C. (2018). *Magic Quadrant for IT Service Management Tools*. Abgerufen von https://www.gartner.com/document/3886969

Govindji, S., Peko, G., & Sundaram, D. (2018). A Context Adaptive Framework for IT Governance, Risk, Compliance and Security. In P. Cong Vinh, N. Ha Huy

Cuong, & E. Vassev (Hrsg.), *Context-Aware Systems and Applications, and Nature of Computation and Communication* (S. 14–24). Springer International Publishing.

Hanudelova, J., & Prochazkova, L. (2018). Organizational Service Management as an Umbrella for Information Business. In N. Kryvinska & M. Gregus (Hrsg.), *Agile Information Business: Exploring Managerial Implications* (S. 177–216). https://doi.org/10.1007/978-981-10-3358-2_6

Hardy, C., & Leonard, J. (2011). Governance, risk and compliance (GRC): Conceptual muddle and technological tangle. *ACIS 2011 Proceedings*. Abgerufen von https://aisel.aisnet.org/acis2011/42

Heiniger, B. (2018). KMU trifft das neue EU-Gesetz besonders hart. *Handelszeitung*. Abgerufen von https://www.handelszeitung.ch/unternehmen/das-neue-eu-gesetz-trifft-kmu-besonders-hart

Hunnebeck, L. (2011). *ITIL Service Design: 2011* (2 edition). London: The Stationery Office.

Hunziker, S., Renggli, S., & Fallegger, M. (2018a). Einleitung. In S. Hunziker, S. Renggli, & M. Fallegger (Hrsg.), *Interne Kontrollsysteme im Finanzbereich: Wirksame und effiziente Steuerung, Kontrolle und Überwachung* (S. 1–2). https://doi.org/10.1007/978-3-658-22982-5_1

Hunziker, S., Renggli, S., & Fallegger, M. (2018b). Grundlagen zum IKS. In S. Hunziker, S. Renggli, & M. Fallegger (Hrsg.), *Interne Kontrollsysteme im Finanzbereich: Wirksame und effiziente Steuerung, Kontrolle und Überwachung* (S. 3–11). https://doi.org/10.1007/978-3-658-22982-5_2

ISACA. (2012). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows, Ill: ISACA.

ISACA. (2018). COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution. Isaca.

Ivanti. (2019). Ivanti Service Manager Documentation. Abgerufen von https://help.ivanti.com/ht/help/en_US/ISM/2019.1/admin/Content/Common/LandingPage.htm

Johannsen, W., & Goeken, M. (2011). Referenzmodelle für IT-Governance: Methodische Unterstützung der Unternehmens-IT mit COBIT, ITIL & Co (2. Aktual.). Heidelberg: dpunkt Verlag.

Knoll, M. (2017). IT-Risikomanagement im Zeitalter der Digitalisierung. *HMD Praxis der Wirtschaftsinformatik*, *54*(1), 4–20. https://doi.org/10.1365/s40702-017-0287-4

Knoll, M., & Strahringer, S. (2017). IT-GRC-Management im Zeitalter der Digitalisierung. In M. Knoll & S. Strahringer (Hrsg.), *IT-GRC-Management – Governance, Risk und Compliance: Grundlagen und Anwendungen* (S. 1–24). https://doi.org/10.1007/978-3-658-20059-6_1

Kraft, R., & Stöwer, M. (2017). IT-Risikomanagement für Produktionssysteme – Basis zur Gestaltung sicherer Fertigungsprozesse. In M. Knoll & S. Strahringer (Hrsg.), *IT-GRC-Management – Governance, Risk und Compliance: Grundlagen und Anwendungen* (S. 97–111). https://doi.org/10.1007/978-3-658-20059-6_7

Lindner, D., & Leyh, C. (2019). Digitalisierung von KMU – Fragestellungen, Handlungsempfehlungen sowie Implikationen für IT-Organisation und IT-Servicemanagement. *HMD Praxis der Wirtschaftsinformatik*. https://doi.org/10.1365/s40702-019-00502-z

Lloyd, V. (2011). *ITIL Continual Service Improvement: 2011* (2011 ed. edition). London: The Stationery Office.

Marekfia, W., & Nissen, V. (2009). *Strategisches GRC-Management - Grundzüge eines konzeptionellen Bezugsrahmens*. Abgerufen von https://www.db-thueringen.de/receive/dbt_mods_00014396

Marrone, M., & Kolbe, L. M. (2011). Einfluss von IT-Service-Management-Frameworks auf die IT-Organisation. *WIRTSCHAFTSINFORMATIK*, *53*(1), 5–19. https://doi.org/10.1007/s11576-010-0257-8

Mayer, N., Barafort, B., Picard, M., & Cortina, S. (2015). An ISO Compliant and Integrated Model for IT GRC (Governance, Risk Management and Compliance). In R. V. O'Connor, M. Umay Akkaya, K. Kemaneci, M. Yilmaz, A. Poth, & R.

Messnarz (Hrsg.), *Systems, Software and Services Process Improvement* (S. 87–99). Springer International Publishing.

Moeller, R. R. (2013). Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL. Hoboken, NJ: Wiley.

Percheiro, I., Almeida, R., Pinto, P. L., & da Silva, M. M. (2017). Towards Conceptual Meta-Modeling of ITIL and COBIT 5. In M. Themistocleous & V. Morabito (Hrsg.), *Information Systems* (S. 478–491). Springer International Publishing.

PricewaterhouseCoopers. (2005). 8th Annual Global CEO Survey: Bold Ambitions, Careful Choices. PricewaterhouseCoopers.

Pröhl, T., & Zarnekow, R. (2019). Die kurze Geschichte des IT-Servicemanagement: Themen und Fragestellungen im Wandel der Zeit. *HMD Praxis der Wirtschaftsinformatik*. https://doi.org/10.1365/s40702-019-00497-7

Racz, N., Weippl, E., & Bonazzi, R. (2011). IT Governance, Risk & Compliance (GRC) Status Quo and Integration: An Explorative Industry Case Study. *Proceedings of the 2011 IEEE World Congress on Services*, 429–436. https://doi.org/10.1109/SERVICES.2011.78

Racz, N., Weippl, E., & Seufert, A. (2010). A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC). In B. De Decker & I. Schaumüller-Bichl (Hrsg.), *Communications and Multimedia Security* (S. 106–117). Springer Berlin Heidelberg.

Rance, S. (2011). *ITIL Service Transition: 2011* (2011 ed. edition). London: The Stationery Office.

Rouhani, S. (2017). A fuzzy superiority and inferiority ranking based approach for IT service management software selection. *Kybernetes*, *46*(4), 728–746. https://doi.org/10.1108/K-05-2016-0116

Rouhani, S., & Ravasan, A. Z. (2014). A Fuzzy TOPSIS based Approach for ITSM Software Selection: *International Journal of IT/Business Alignment and Governance*, *5*(2), 1–26. https://doi.org/10.4018/ijitbag.2014070101

Schlarman, S. (2009). What ITIL can Teach IT-GRC. *EDPACS*, *40*(2), 8–18. https://doi.org/10.1080/07366980903340012

Schneider, T. (2018). Ziele und Planung. In T. Schneider (Hrsg.), *Wirkungsvolle Compliance: Mit praxiserprobten Maßnahmen zur erfolgreichen Umsetzung* (S. 45–56). https://doi.org/10.1007/978-3-662-55941-3_6

Schomann, M., & Röder, S. (2008). Entwicklung eines kennzahlenbasierten Steuerungssystems für IT-Service-Management-Prozesse nach ITIL. In F. Keuper & B. Hogenschurz (Hrsg.), *Sales & Service: Management, Marketing, Promotion und Performance* (S. 323–359). https://doi.org/10.1007/978-3-8349-9591-9_15

Schweizer, M. (2017). Governance, Risk und Compliance (GRC) – Freund oder Feind von IT Service Management? - Digicomp Blog. Abgerufen von https://www.digicomp.ch/blog/2017/02/17/grc-freund-oder-feind-von-itsm

ServiceNow. (2019a). ServiceNow Reports Record Fourth Quarter and Fiscal Year 2018 Financial Results. Abgerufen von https://www.servicenow.com/company/media/press-room/servicenow-reports-record-fourth-quarter-and-fiscal-year-2018-financial-results.html

ServiceNow. (2019b, Mai 1). ServiceNow Governance, Risk, and Compliance Documentation. Abgerufen von https://docs.servicenow.com/bundle/madrid-governance-risk-compliance

Söllner, D., & Drescher, M. (2019). Service Management in der Ära von Agile und DevOps. *HMD Praxis der Wirtschaftsinformatik*. https://doi.org/10.1365/s40702-019-00504-x

Spalding, G. (2019). *What's New in ITIL 4? Key Changes, Implications, and Practical Guidance*. Abgerufen von https://www.brighttalk.com/webcast/14485/347709

Steinberg, R. A. (2011). *ITIL Service Operation: 2011* (2011 ed. edition). London: The Stationery Office.

Teubner, A., & Remfert, C. (2017). Giving IT Services a Theoretical Backing. In S. Yamamoto (Hrsg.), *Human Interface and the Management of Information: Information, Knowledge and Interaction Design* (S. 448–468). Springer International Publishing.

Urbach, N., & Gschwendtner, M. (2012). *IT-Governance in der Unternehmenspraxis*. EBS Business School und Horváth & Partners Management Consultants.

Wiedenhofer, A. (2017). Verbesserung des Wertbeitrags von IT-Organisationen – Empirische Handlungsempfehlungen. In M. Knoll & S. Strahringer (Hrsg.), *IT-GRC-Management – Governance, Risk und Compliance: Grundlagen und Anwendungen* (S. 51–64). https://doi.org/10.1007/978-3-658-20059-6_4